地域におけるデータ利活用のための
コード決済情報等の適正な取扱に関する
ガイドライン

2021 年 **4** 月 **27** 日

一般社団法人キャッシュレス推進協議会

目次

1　はじめに

本書は、総務省「地域における決済情報等の利活用に係る調査」を踏まえて作成された「決済事業者等からの決済情報取得にかかる標準ガイドライン」と「地域におけるデータ利活用のためのコード決済情報等の適正な取扱に関するガイドライン」のうち、後者の「地域におけるデータ利活用のためのコード決済情報等の適正な取扱に関するガイドライン」である。

政府は、「成長戦略フォローアップ」（令和元年 6 月 21 日閣議決定）において、2025 年 6 月までにキャッシュレス決済比率を倍増し、4 割程度とすることを目指している。新たなデータの蓄積や、現金処理コストの削減による店舗の生産性向上、消費者の支払いにおける利便性向上等を実現する観点から、キャッシュレス化の推進を掲げ、その更なる進展が期待されている。

キャッシュレス決済のうち、モバイル端末を用いたバーコード・QR コード[1]決済（以下、コード決済という）は、その低廉な手数料等から地域の店舗にとって導入が容易であり、地域のキャッシュレス化を推進する上で効果的な決済手段である。

総務省は「コード決済に関する統一技術仕様ガイドライン」[2]に基づき、統一 QR「JPQR」を活用した実証事業を「統一 QR『JPQR』普及事業」として令和元年度に実施した。同事業において、小規模店舗を含め「JPQR」を活用したコード決済を地域で面的に導入するためのモデルを確立し、地域におけるキャッシュレス決済比率の向上を後押しした。

既にコード決済の導入が進んでいる地域では、店舗の生産性向上、消費者の支払いにおける利便性向上等を実現しており、店舗や消費者はキャッシュレス化による更なるメリットを期待している。例えば、店舗は決済金額・決済日時等を活用することで需要傾向を把握しやすくなり、消費者は個人の消費行動に併せて店舗からきめ細かいサービスを受けられるようになる。このように店舗や消費者にとっての継続的なメリットをよりわかりやすく提示することが地域全体にキャッシュレス化、決済データの利活用を広げる上で重要となる。

しかしながら、現状では新たなデータの蓄積や決済データの利活用は進んでいない。その理由の一つとして、決済事業者や店舗が分断してデータを保有し、異なる事業者間

[1] QR コード®は、株式会社デンソーウェーブの登録商標である。
[2]一般社団法人キャッシュレス推進協議会（以下、キャッシュレス推進協議会という）公表の Ver2.0（公表日令和 2 年 4 月 27 日）
参照 URL：https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2020/04/MPM_Guideline_2.0.pdf

で共有しづらいことが挙げられる。決済データを授受する API 等、決済事業者とデータ利活用を推進したい第三者との間で決済データ連携に係るルールがなく、結果として決済データを流通させづらい状況になっている。

総務省は、決済データの利活用に向けて、決済事業者等から決済データを取得する際の API 接続、及び決済事業者の持つ決済データや店舗の持つ購買データを扱うためのルール作りを促すために、令和 2 年度「地域における決済情報等の利活用に係る調査」を実施した。

本調査では、決済データ等を地域で利活用する場面を仮説的に設定したモデル事業に取組み、それぞれのケースにおいて、決済事業者とデータ利活用を推進したい第三者の間で決済データ等の連携を行う際に必要な要件の洗い出しを実施した。また、洗い出した要件を基に、決済事業者等から決済データを取得する際のルール作りや、決済事業者の持つ決済データ、店舗の持つ購買データ、及びコード決済を利用した利用者の属性データ（以下、利用者属性データという）を第三者が扱うためのルール作りを実施した。モデル事業を通して作成したルールをガイドラインとしてまとめる際には、キャッシュレス推進協議会と連携しながら作成した。

仮説的に設定したモデル事業内容は、地域における決済データの利活用に向け、決済データの発生源である決済事業者、店舗や消費者、自治体・公共機関等にとって長期的なインセンティブ創出に繋がるように設計し推進した。加えて本書は、モデル事業実施地域以外において決済データや購買データ等の利活用を試みる際の参考となるように設計したガイドラインである。

（参考）

1. 地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドライン

コード決済に係る既存の決済事業者、及び今後事業を開始する決済事業者や地域ウォレット事業者[3]（以下、決済事業者等という）が、データを利活用する基盤（以下、データ利活用基盤という）に対して決済データ等を連携する際のルール作りを目的としたガイドラインである。決済事業者等が、決済データ等を連携してデータを利活用する基盤を整えるための指針の一つとして位置づけられる。総務省「地域における決済情

[3] 地域ウォレット事業者とは、地域ウォレットを提供する事業者を指す。地域ウォレットとは、地域利用者にとって、その地域の中での暮らしや体験のために身近にあると役に立つものが「財布」のようにまとめて管理されているスマートフォンアプリケーションと本書では定義する。詳細は「地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドライン」の「1.3　位置付け」を参照

報等の利活用に係る調査」におけるモデル事業を通じて、必要とされる API 等の仕様標準を検証し作成された。

2. 地域におけるデータ利活用のためのコード決済情報等の適正な取扱に関するガイドライン

データ利活用に係る各関連事業者（自治体、データ利活用基盤の運営主体、決済事業者、店舗等）（以下、各関連事業者という）が決済データや購買データを取扱い、利活用する際のルール作りを目的としたガイドラインである。各関連事業者が決済データ等を連携して、データ利活用基盤を整えるための指針の一つとして位置づけられる。総務省「地域における決済情報等の利活用に係る調査」におけるモデル事業を通じて、決済データを取扱う上での望ましい運用上のルール（同意取得のあり方、データフロー、セキュリティ要件等）を検証し作成された。

1.1 データ利活用の必要性、キャッシュレス化の意義について

政府は「まち・ひと・しごと創生長期ビジョン（令和元年改訂版）及び 第 2 期『まち・ひと・しごと創生総合戦略』」[4]にて、国として目指すべき大きな柱として、「将来にわたって活力ある地域社会の実現」を掲げており、地域社会の課題解決を中心に据えている。また、総務省は「地方公共団体におけるデータ利活用ガイドブック Ver.2.0」[5]にて、地方公共団体が直面する地域社会の課題解決手段として、データ利活用の必要性を表明している。しかし、地方公共団体におけるデータ利活用においては、紙媒体による情報管理、データ形式の不統一化、各種データの共同管理の未実施等多くの課題がある。地域社会の課題解決手段としてデータを活用するためには、まず取扱うデータを取得し、整理する所から始める必要がある。決済データにおいては、キャッシュレス化がこのデータ取得と整理をするための後押しとなり得る。

キャッシュレス化とデータ利活用が地域全体に広がると、次のような社会課題解決の糸口がみつかることが期待される。

- 決済データや購買データと周辺情報を組み合わせることで、消費者の見える化ができ、買い物弱者、交通弱者の支援等に役立つサービスが生まれる。それにより消費者の生活が変化し、それが課題解決の糸口になる。実際に幾つかの地方公共団体

[4] まち・ひと・しごと創生長期ビジョン（令和元年改訂版）及び 第 2 期「まち・ひと・しごと創生総合戦略」が閣議決定（公表日令和元年 12 月 20 日）
参照 URL：https://www.kantei.go.jp/jp/singi/sousei/info/pdf/r1-12-20-gaiyou.pdf
[5] 総務省情報流通行政局公表 地方公共団体におけるデータ利活用ガイドブック Ver.2.0（公表日令和元年 5 月 21 日）参照 URL：https://www.soumu.go.jp/main_content/000620312.pdf

では、キャッシュレス化に取組み、「地域の稼ぐチカラの向上」「新しいサービスの提供」等で成果を創出することに成功している[6]。

- 決済データや観光資源の情報と観光客の属性情報を組み合わせることで、特定地区に偏る混雑の解消や、人流の分散が見込める。それにより観光客の満足度が向上するだけでなく、周辺地域への送客や注目度が低かった観光資源の発掘等に繋がり、観光地が抱える課題解決の糸口となる。
- 自治体が中心となり、貨幣とは異なる地域内限定のポイント等、独自通貨を作ることで、地域内の消費や流通を活性化させる施策が見込める。それを持続することにより、 地域の経済・コミュニティの付加価値向上に繋がり、過疎化が進む地域が抱える課題解決の糸口となる。

1.2 地域のデータ利活用を取り巻く課題について

前項にて地域の社会課題解決や地域活性化のためにデータ利活用の有効性を示したが、データの利活用推進にあたり現状では大きく三つの課題が存在する。自治体等がこれらの課題に対応する負荷を回避すべくデータ利活用を断念すると、結果として地域の利便性が損なわれる可能性がある。

本書は、こういった事態にならぬよう、決済事業者とデータ利活用を推進したい第三者との間での決済データ連携に係るルールや、決済データや購買データを取扱う際の考慮点をガイドラインとして定め、自治体等がデータ利活用に取り組む手続の複雑化を防ぐことを図るものである。

1.2.1 データの所有者と所在の課題

一般的に複数種類のデータを組み合わせることで新たな事象を発見できることがある。決済データを例にとると、購買商品の情報を含む購買データやコード決済を利用した際の利用者属性データと突合することで消費行動を類型化できる等、新たな価値を生む見込みがある。しかし現状では、決済データは決済事業者に、購買データは店舗に存在し、利用者属性データは消費者のスマートフォンアプリ等に利用が制限された状態で存在している。データの所有者が異なり所在も分散しているため、複数種類のデータを組み合わせて活用することは困難である。

---

[6] 経済産業省公表キャッシュレス・ビジョン外伝 キャッシュレスから始めるデータ利活用 ～地域と中小企業編～（令和２年３月公表）
参照 URL：
https://www.meti.go.jp/policy/mono_info_service/cashless/cashless_sub/cashless_data_utilization_report.pdf

1.2.2 決済データ等の取得に伴う課題

前項の通り、現状では、データの所有者が異なり所在も分散しているため、仮に自治体や地域の事業者（自治体の外郭団体等）（以下、自治体等という）が主体となって地域のデータ利活用を行う際には、決済事業者や店舗とデータを取得する契約を締結する必要がある。現状では共通の契約や接続（以下、手続という）が確立されておらず[7]、自治体等が複数の決済事業者や店舗からデータを取得する際には、各社と個別の手続をする必要がある。そのため自治体等にも混乱や誤解に基づく不利益が生じることが懸念される。

1.2.3 決済データ等の取扱いに関する課題

決済データや購買データ、利用者属性データ等を利活用する者は、それらのデータの利用目的等について消費者へ説明を丁寧に行い、データの内容や利活用の方法によっては同意を取得する必要がある。(詳細は「4.8 個人情報保護法観点で遵守すべきこと」を参照) また、それらのデータを格納、加工する場となるデータ利活用基盤にはセキュアな管理が求められ、第三者へのセキュアな伝送が求められる。このように情報の取扱いに関して満たすべき法的・技術的水準が高いため、自治体等が独自に取り組むことは困難である。

1.3 本書の位置づけ

本書は、前項に挙げた 1.2.3 決済データ等の取扱いに関する課題を解決し、データ利活用を行う者が、決済データや購買データ、利用者属性データ等を適切に扱い、データ連携における手続等を円滑に進めるための指針である。決済データ等を地域で利活用する場面を想定したモデル事業を行い、モデル事業を通じて有効性が認められた解決策等を指針として提示する。

次年度以降、他地域にて決済情報等の利活用の取り組みを横展開できるように汎用化し、経済活性化等、地域社会の課題解決に寄与するものである。

1.4 適用範囲

データの流通・利活用は、大きな期待をもって取り組まれている分野である。利活用されるデータの種類や規模も多岐に渡る中で、特に個人データを含むデータ利活用に

[7] Fintech 等事業者向けの取得方法については、キャッシュレス推進協議会にてガイドラインを策定済
参照 URL：https://www.paymentsjapan.or.jp/wordpress/wp-content/uploads/2020/12/API_Guideline_Ver2.1.pdf

関しては、セキュリティ面を中心により慎重な取扱いが必要な領域となる。個人データを取扱わない形でのデータ利活用もあるため、取扱うデータの範囲を検討する際には個人データの取得要否も含めて検証する必要がある。本書では、決済データや購買データ等を地域で利活用することを前提としており、スマートフォンアプリ等から利用者本人のデータを取得時に本人認証が必要となる等、取扱う決済データ等の中には個人データ、及び他の情報と照合することで個人を特定できてしまうデータを含むことが多いと想定される。そのため、本書の適用範囲は個人データを含むデータ利活用とし、データを適切に取扱うための指針を提示する。（図表 1 参照）

また、個人情報を取得していても、個人情報を全く保管しないケースに関してなどは本書の記載の限りではない。

図表 1　取扱いデータにおける本書での取扱い

データ取得	データ保管・分析	利活用者に受け渡すデータ	本書での取扱い
個人情報を含む	個人情報を含む	個人情報を含む	－
		個人情報を含まない	○
	個人情報を含まない	－	－
個人情報を含まない	－	－	－

個人データを含むデータ利活用を行う際には、取得した個人データが漏えい等をした場合のリスクを最小限に抑えるための工夫をすることも重要である。利活用する目的によっては、必ずしも個人データのすべてをそのまま保管・利活用する必要がないものもあると考えられるため、部分的であれ必要に応じて個人が特定できないような形にデータを加工する等[8]、個人データ取扱いの手順や管理方法について、事前に十分な検討・確認をすることが望ましい。本書で取扱う個人データとは、主に決済データ、購買データ、利用者属性データを突合したものを指すが、実務で取扱った際には、突合した個人データを加工・分析し、データ利活用に係る各関連事業者へは個人を特定できない統計情報にして受け渡した。今回は統計情報を受け渡しているが、今後個人データを含む情報を提供対象とする場合には、必要に応じてガイドラインの見直しを行う。

以下の図表 2 において、地域のデータ利活用を実現するにあたって、作業手順と各地域のデータ利活用に係る各関連事業者が行う主な活動を示す。データ利活用を実施

[8] データの加工には幅があり、統計情報化、匿名加工、仮名加工等、利用目的（データ分析、データ利活用）が達成できる範囲において加工の程度を決める。一人一人の単位でなく分析すればよいものは、統計情報化や、匿名加工にて対応できるが、今回のように決済のトランザクションと一人一人の行動を組み合わせての分析が必要な場合では仮名加工情報が適切と判断した。

するときの作業手順は、大きく 5 ステップで表すことができ、本書では、各地域で手順を共通化しやすいステップ 3～5 の対象箇所について記載する。

図表 2　データ利活用を実施するときの作業手順

作業手順	本書の対象	各地域のデータ利活用に係る各関連事業者が行う主な活動
ステップ 1 課題を設定する	-	対象となる地域で解決したい課題を洗い出し、優先度をつける
ステップ 2 仮説を検討する	-	課題が発生している原因を調査する
		解決策を検討する
		検証方法を検討する、必要に応じて目標値設定等をする
ステップ 3 データを集める	-	データ収集及び、収集したデータを突合する（API の活用等による連携方式）　※「地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドライン」にて定義
	●	データ収集及び、収集したデータを突合する （ユーザ合意や、契約等）
	●	分析を意識したデータ取得項目の整理をする
ステップ 4 データを分析する	●	分析のためのデータの保管から破棄まで管理する
	-	具体的な分析手法を検討する
ステップ 5 データを利活用する	●	データ（今回は統計情報）の生成方法や受け渡しにおける留意点を確認した上で、地域の社会課題解決や活性化につなげる

尚、「4 活用編」「5 安全管理措置」において、データを集める際の注意点、及びその方針や手法を記載する。

図表 3　データを集める際の注意点等

方針や手法	記載している項番
データを集める際のユーザ同意や、契約について	4.4 以降にモデル事業事例を記載する。 主に「ステークホルダリスト」、「ビジネス関係図」、「データフローシーケンス」を参照のこと
データを集めた後、データ分析するための加工や、契約について	4.4 以降にモデル事業事例を記載する。 主に「ビジネス関係図」、「データリソースマップ」、「トラストリソースマップ」を参照のこと
データ保管方法や、データ使用後の破棄の仕方について	5 安全管理措置を参照のこと
データ受け渡し時の注意点について	4.4 以降にモデル事業事例を記載する。 「ビジネス関係図」、「データリソースマップ」を参照のこと

1.5 本書の想定読者

本書では、地域のデータ利活用を推進する際に、データ利活用に係る各関連事業者等の役割（以下、ロール[9]という）を五つ定義[10]した。そのうちデータ利活用推進主体、データ利活用基盤システム運用者、データ分析者のロールを担うものを読者とする。参考として、図表 4 に各ロールに該当することが想定される各関連事業者等の例を記載する。尚、一つの事業者が複数のロールを担う場合もある。

また、本書で示す指針、及びモデル事業を通じて有効性が認められた解決策は、読者が決済情報等を地域で利活用する際の参考とすることを目的としており、強制力を持つものではない。しかしながら、本書はデータ利活用、及び個人情報の取扱い等に関する高い専門知識を有する幅広い関係者による検討を踏まえて作成されたものであり、本書の目的達成のためにも、事業者の特性や規模に応じ可能な限り対応することが望まれる。

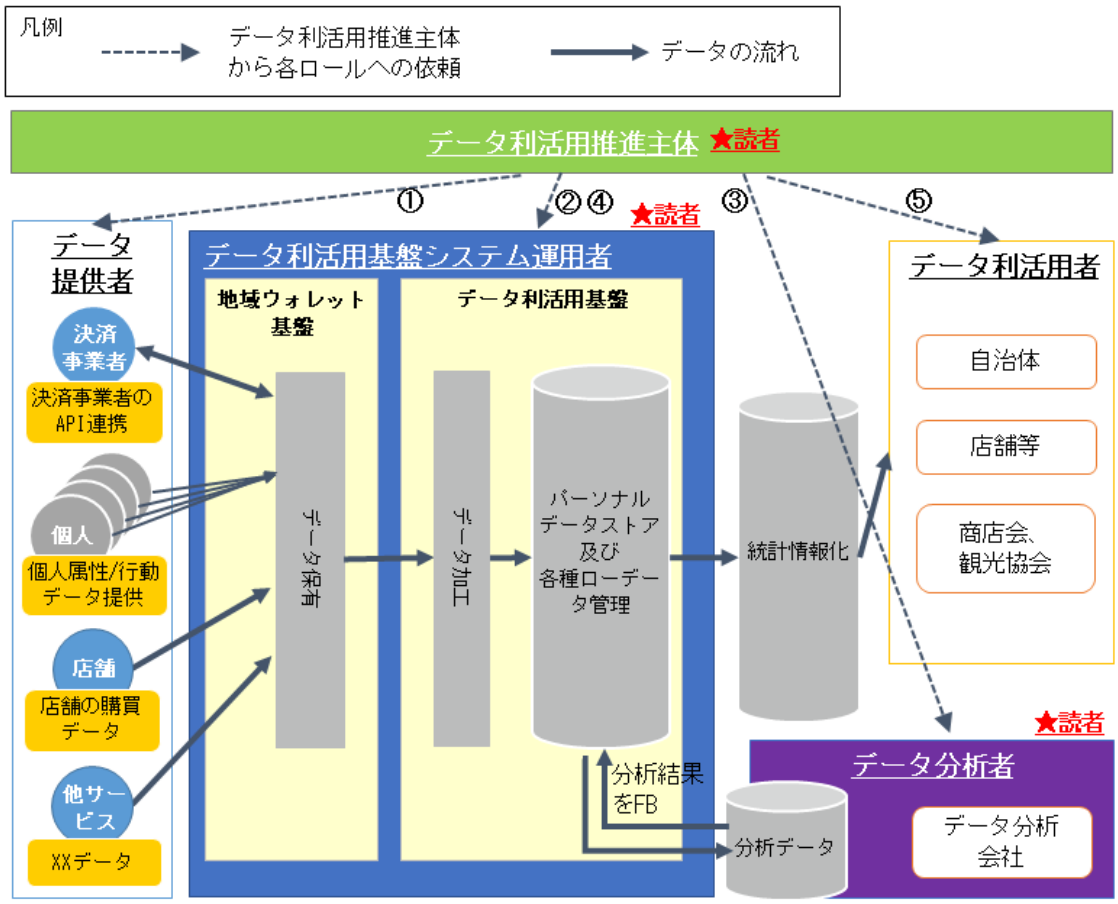
[9] ロール名は現時点のものであり、今後の文書の改訂時等に変更する場合がある。
[10] ロールの定義は現時点のものであり、今後の文書の改訂時等に変更する場合がある。

図表 4　データ利活用におけるロールと想定される各関連事業者

ロール名	個人情報取扱有無	役割	想定される各関連事業者	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
データ利活用推進主体	有	課題を解決するための仮説検討、及びその推進を行う団体や事業者等。	データ利活用する意志がある自治体・事業者（自治体の外郭団体、商工会議所、交通事業者等）	地域ウォレット事業者が該当する場合もある
データ利活用基盤システム運用者	有	データ利活用基盤を提供し、データ保持、及び加工をする事業者等。	個人情報を扱うサービスを行っている事業者（決済事業者、スーパー、金融機関、サービス提供ベンダー等）	地域ウォレット事業者
データ分析者	有	データ利活用基盤にて共同利用するデータの分析を担う団体や事業者等。	データ分析を行う事業者、若しくはデータ利活用推進主体やデータ利活用基盤システム運用者が兼務	
データ提供者	有	個人データ等を提供する事業者等。	個人情報を扱うサービスを行っている事業者（決済事業者、サービス提供ベンダー、銀行、スーパー等）	決済事業者、店舗
データ利活用者	無	利活用データの提供（本書では統計データの受け渡し）を受ける団体や事業者等。	自治体、商工会議所、店舗等	

データ利活用におけるロール間の関係を図表 5 に記載する。データ利活用推進主体が、他のロールとの接点を持ちながらデータ利活用の実行を担う。

図表 5　データ利活用推進主体と他ロールの関係



① データ利活用推進主体が、データ提供者に対して、提供依頼を実施

② データ利活用推進主体が、データ利活用基盤システム運用者に対して、データ加工要件等を提示

③ データ利活用推進主体が、データ分析者に対して、データ分析を依頼

④ データ利活用推進主体が、データ分析者が実施した分析結果をもとにデータ利活用基盤システム運用者に対して、統計情報化を依頼

⑤ データ利活用推進主体が、データ利活用者に対して、分析結果から得られた統計情報を報告説明

1.6 本書の構成

本書は、次章以降で導入編と活用編にて構成される。

導入編では、データ利活用を行う際に最初に読むべきものとして、「2 決済情報や購買情報の取扱いに関する基本理念」及び「3 関連法制」においてガイドラインを活用するための前提となる知識や考え方等について解説する。

活用編では、実際に利活用する際に読むべきものとして、「4 活用編」及び「5 安全管理措置」にてデータを格納し分析・加工する手法や、運用上の留意点等について解説する。

図表 6　本書の構成

分類	利用形態	章
導入編	ガイドラインを活用するための前提となる知識や考え方を理解する際に参照する	2 決済情報や購買情報の取扱いに関する基本理念 2.1 関連法令の遵守 2.2 個人情報の定義 2.3 複数ステークホルダ間で個人データを扱う場合 2.4 個人情報保護法の改正
		3 関連法制 3.1 全体像 3.2 行政規制（個人情報保護法） 3.3 民事ルール（契約法）
活用編	実際にデータを格納し、分析・加工を経て、データの利活用をする際に参照する	4 活用編 4.1 活用編の位置づけ 4.2 ユースケースシナリオテンプレートの利用手順 4.3 ユースケースシナリオテンプレートの記載方法について 4.4 ユースケースシナリオテンプレートの活用事例 4.5 生活支援モデルの例 4.6 観光支援モデルの例 4.7 交通支援モデルの例 4.8 個人情報保護法観点で遵守すべきこと
		5 安全管理措置 5.1 安全管理措置について 5.2 安全管理措置の検討手順 5.3 安全管理措置の内容 5.4 安全管理措置の内容（データ利活用推進主体及び、データ分析者向け）

1.7 本書の改訂方針

本書の記載内容に関しては、今後発生する課題、及び法規制や社会環境の変化等に応じて改訂が必要である。キャッシュレス推進協議会は適時、本書の改訂についての検討を行うものとする。

2 決済情報や購買情報の取扱いに関する基本理念

本章では、決済データや購買データを取扱う各関連事業者が、その事業形態や、図表 4 で示したデータ利活用におけるロールに関わらず、理解と配慮をすべき基本的な理念、及び本書を読み進める上で前提となる考え方を記載する。

2.1 関連法令の遵守

2.1.1 データ利活用に関連する主な論点

地域のデータ利活用を実現するにあたり、各関連事業者は、関連法令を遵守しなければならない。その中でも、決済情報等に含まれる個人情報の取扱いについては、「個人情報の保護に関する法律」[11]（以下、個人情報保護法という）を中心に、関連する法令、政令、規則、ガイドライン等を遵守する必要がある。

2.1.2 本書での対応

本書では、個人情報保護法及び個人情報保護委員会が定める「個人情報の保護に関する法律についてのガイドライン（通則編）」[12]（以下、「通則編」という）を拠りどころとして、各関連事業者が決済情報等を取扱う際に特に考慮すべき点について記載する。尚、「5 安全管理措置」については、本書の想定読者である 3 つのロール（データ利活用推進主体、データ利活用基盤システム運用者、データ分析者）のうち、決済事業者と接続し、決済データを直接取扱うデータ利活用基盤システム運用者は、個人情報保護委員会及び金融庁が定める「金融分野における個人情報保護法に関するガイドライン」及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」を拠りどころとして記載する[13]。

また、モデル事業実施地域以外で決済データや購買データ等の利活用を試みる際の参考となるように、今回のモデル事業での取組みを併せて記載する。但し、本書は、決済データ等の取扱いに関連する事項を述べるものであり、本書を実践することでデータ利活用事業全体における関連法令の適合性を保証するものではない。従って、データ

---

[11] 「平成 15 年法律第 57 号」に基づく現行版（令和 2 年 12 月 12 日時点）
参照 URL：https://www.ppc.go.jp/files/pdf/201212_personal_law.pdf
[12] 個人情報保護委員会公表の現行版（平成 28 年 11 月公表、令和 3 年 1 月一部改正）
参照 URL：https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf
[13] この他に、具体的な事例を本書で記載するに当たり「（別添）特定個人情報に関する安全管理措置（事業者編）」も参照した。
参照 URL：https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha.pdf

利活用に係る各関連事業者は自身の事業と照らし、自己の責任と負担において関連法令を調査し、これらを遵守されたい。

2.2 個人情報の定義

2.2.1 データ利活用に関連する主な論点

地域のデータ利活用を実現するにあたり、個人情報を取扱う各関連事業者は、個人情報とは何かを理解し、各事業において個人情報の定義に該当する範囲を明確にする必要がある。その上で、個人情報については関連法令を遵守するとともに、厳密には個人情報の定義には該当しないがそれに類する情報について、どのように取扱うか検討することとなる。

個人情報保護法では、「個人情報[14]」、「個人データ[15]」、「保有個人データ[16]」、「要配慮個人情報[17]」等を定義して、個人情報取扱事業者に課される義務は、上記の定義された情報に応じて定められているため、注意が必要である。

2.2.2 本書での対応

本書では、決済データ等を地域で利活用する際に特に考慮が必要となる事項について、モデル事業での具体例を踏まえて記載する。

各関連事業者が取扱う決済データ等やスマートフォンアプリ（地域ウォレット）等から取得する情報には、それ自体で、「特定の個人を識別することができる」場合がある。またそうでなくとも、法第 2 条第 1 項第 1 号が示す「他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるもの」が含まれる場合も多いと想定される[18]。従って、各関連事業者が地域のデータ利活用を行う際には、取得するデータや加工したデータ自体の確認だけでなく、容易に照合できるデータの有無を把握した上で、個人情報に該当するか確認し、その取扱いを決定する際に考慮する必要がある。

---

[14] 個人情報の法的な定義については、通則編（2-1 個人情報、2-2 個人識別符号）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf
[15] 個人データの法的な定義については、通則編（2-6 個人データ）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf
[16] 保有個人データの法的な定義については、通則編（2-7 保有個人データ）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf
[17] 要配慮個人情報の法的な定義については、通則編（2-3 要配慮個人情報）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf
[18] 例えば、電話番号、メールアドレス、契約者・端末固有 ID、ログイン ID などが情報単体では個人識別性がない場合でも、契約者の氏名等個人情報と容易に結びつく場合には個人識別性を獲得する。詳細は、総務省公表の「スマートフォン プライバシー イニシアティブ」を参照。
参照 URL：https://www.soumu.go.jp/main_content/000358525.pdf

2.3 複数ステークホルダ間で個人データを扱う場合

2.3.1 データ利活用に関連する主な論点

複数のステークホルダにまたがって決済データや購買データを適切に取扱う上で特に重要と考えられる要素の一つが、どこでどのような個人情報が取得され、その個人情報がどこに移転され活用されているかといった全体像を明確にすることである。

尚、個人情報保護法では、個人情報取扱事業者が自らの保持する個人データを他のステークホルダへ受け渡すには、本人の同意の下での「第三者提供」が原則であるが、他の方法として、「委託」「事業の承継」「共同利用」「オプトアウト」等もある（詳細は本書「4.8.4 個人データの第三者への提供」を参照）。それぞれの方法により、データの提供元及び提供先に課される義務も異なる。

図表 7　データ受け渡しの種類

受け渡しの種類	概要（通則編より一部抜粋）
委託 （法第 23 条第 5 項第 1 号）	個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが受け渡される場合
事業の承継 （法第 23 条第 5 項第 2 号）	合併その他の事由による事業の承継に伴って個人データが受け渡される場合
共同利用 （法第 23 条第 5 項第 3 号）	特定の者との間で共同して利用される個人データが当該特定の者に受け渡される場合であって、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき
第三者提供 （法第 23 条～第 26 条）	委託、事業の承継、共同利用以外の方法で、個人データが第三者へ提供される場合

2.3.2 本書での対応

地域のデータ利活用をするためには、複数のステークホルダ間で個人データの受け渡しを行う場面があると想定されるが、その際には、当該受け渡しの目的や実態などを踏まえて、事業の特性に適した形態で受け渡し、それぞれの形態において提供元、及び提供先に課される義務を履行する必要がある。委託、事業の承継、共同利用は、あくまで本人との関係において提供主体である個人情報取扱事業者と一体のものとして取扱うことに合理性があるがゆえに、個人データの受け渡しに本人の同意が不要であるとされていることに留意する必要がある。例えば委託においては、委託先は、委託元から受託した業務の範囲内で個人データを取扱う必要があり、委託元の利用目的の達成を

離れて、委託先自らの利用目的で受け渡された個人データを利用することはできない。また共同利用においては、上記の趣旨からして、共同利用する者の範囲を広範に設定することは適切ではない場合がある。そして、通常の第三者提供においては、本人の同意を得なければならない。本書では、「4.8 個人情報保護法観点で遵守すべきこと」にてそれぞれの形態において考慮すべき事項を記載する。

また、モデル事業実施地域以外で決済データや購買データ等の利活用を試みる際の参考となるように、今回のモデル事業での取組みを併せて記載する。今回のモデル事業においては、複数のステークホルダが特定の事業を共同で推進することを目的として、個人データの共同利用を行ったが、その際には共同利用の責任を持つ者として共同利用する事業者のうち 1 社を管理責任者と定め、個人データがどこに移転され活用されるかを管理した。

2.4 個人情報保護法の改正

2.4.1 データ利活用に関連する主な改正法

個人情報保護法は個人情報保護委員会[19]が所管しており、同委員会が「個人情報の保護に関する基本方針」の策定等を行い、個人情報の保護に関する取組みを推進している。個人情報保護委員会は、個人情報保護法の「いわゆる 3 年ごと見直し」について、平成 31 年 1 月より、実態把握や議論整理等を行い、大綱として公表した（令和元年 12 月 13 日）[20]。そして、令和 2 年 6 月 12 日に「個人情報の保護に関する法律等の一部を改正する法律」[21]（以下、「令和 2 年改正法」という）が公布され、令和 4 年 4 月 1 日に施行される予定である。

① 仮名加工情報

- 令和 2 年改正法において、「個人情報」と「匿名加工情報」の中間的な制度として、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工した個人に関する情報である「仮名加工情報」を創設した
- 仮名加工情報の制度創設の趣旨は、一定の安全性を確保しつつ、データとしての有用性を加工前の個人情報と同等程度に保つことができるように、匿名加工情報に

[19] 個人情報の保護に関する法律（平成 15 年法律第 57 号）に基づき設置された合議制の機関。個人の権利利益を保護するため、個人情報の適正な取扱いの確保を図ることを目的としている。
参照 URL：https://www.ppc.go.jp/
[20] 個人情報保護委員会が「個人情報保護法の 3 年ごと見直し」の内容を取りまとめた文書。「個人情報保護法 いわゆる 3 年ごと見直し 制度改正大綱」（公表日令和元年 12 月 13 日）
参照 URL：https://www.ppc.go.jp/files/pdf/200110_seidokaiseitaiko.pdf
[21] 詳細は個人情報保護員会 HP にて公表
参照 URL：https://www.ppc.go.jp/personalinfo/legal/kaiseihogohou/#3nenminaoshi

比してより簡便な加工により得られる新たな類型を設けることで、イノベーションの促進を図る点にある

- 「匿名加工情報」とは異なり、法令に基づく例外的な場合以外第三者提供することはできない

② 個人関連情報

- 個人関連情報とは、「生存する個人に関する情報であって、個人情報、仮名加工情報及び匿名加工情報のいずれにも該当しないもの」をいう
- （個人関連情報に該当する例：氏名等と結びついていないインターネットの閲覧履歴、位置情報、Cookie 情報等）
- 個人関連情報取扱事業者は、提供先が個人関連情報を個人データとして取得することが想定されるときは、あらかじめ当該個人関連情報に係る本人の同意等が得られていることを確認しないで、当該個人関連情報を提供してはならない

2.4.2 本書での対応

本書では、令和 2 年改正法について、データ利活用に関連する主な論点を、個人情報保護委員会が公表している文書[22]を引用するにとどめ、今後、個人情報保護委員会のガイドライン等と照らし、必要に応じて改訂するものとする。

尚、今回のモデル事業において、共同利用の契約を締結したステークホルダ間で個人データを受け渡す際には、より安全性を高めるために個人データを提供する事業者が仮名加工情報を作成するのと同等の方法により加工して、受け渡しを実施した。また、共同利用の契約を締結していない事業者及び、自治体へ利活用するデータを受け渡す際には、特定の個人との対応関係が排斥された統計情報とすることで個人情報にはあたらないようにした。

22 「改正法に関連する政令・規則等の整備に向けた論点について（仮名加工情報）」（公表日令和 2 年 11 月 27 日）
参照 URL：https://www.ppc.go.jp/files/pdf/201127_kameikakou.pdf
及び、「改正法に関連する政令・規則等の整備に向けた論点について（個人関連情報）」（公表日令和 2 年 11 月 20 日）
参照 URL：https://www.ppc.go.jp/files/pdf/201120_kozinkanren.pdf

3 関連法制

本章では、個人情報保護法の位置づけとともに、決済データや購買データを取扱う各関連事業者が、ステークホルダ間で契約を締結する際に考慮すべき基本的な理念、及び本書を読み進める上で前提となる考え方を記載する。

3.1 全体像

関連法制を整理するにあたり、「消費者委員会消費者法分野におけるルール形成の在り方等検討ワーキング・グループ」[23]の報告書[24]における整理に従い、行政規制と民事ルール（契約法）に分類して本書における考え方を記載する。

尚、当該報告書では、行政規制が「不特定多数者の利益（公益）を実現することを目的として」おり、民事ルール（契約法）が「私人間の個別利益の調整を目的として」いるとされている。

3.2 行政規制（個人情報保護法）

3.2.1 データ利活用に関連する主な論点

個人情報保護法、関連する法律、条例は、現状は民間分野（民間事業者）と公的分野（国の行政機関、独立行政法人等、地方公共団体等）で適用範囲が分かれている[25]。個人情報保護に関連する法令・ガイドライン等のうち、参考となる主要なものを以下に記載する。

① 民間分野に関するもの

- 個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 57 号）

---

[23] 消費者委員会事務局のもと公正な市場を実現するために、中長期的な観点から、消費者法（取引分野）におけるルール形成の在り方及びルールの実効性確保に資する方策並びに行政、事業者（団体）、消費者（団体）等の役割について検討を行った組織

[24] 消費者委員会「消費者法分野におけるルール形成の在り方等検討ワーキング・グループ報告書」（令和元年 6 月公表）
参照 URL：https://www.cao.go.jp/consumer/kabusoshiki/torihiki_rule/doc/201906_torihiki_rule_houkoku.pdf

[25] 令和 3 年 2 月 9 日に「デジタル社会の形成を図るための関係法律の整備に関する法律案」が閣議決定され、個人情報保護法、行政機関個人情報保護法、独立行政法人等個人情報保護法の 3 本の法律を 1 本の法律に統合するとともに、地方公共団体の個人情報保護制度についても統合後の法律において全国的な共通ルールを規定する動きもある。
・個人情報保護員会「官民を通じた個人情報保護制度の見直し」
参照 URL：https://www.ppc.go.jp/personalinfo/minaoshi/
・内閣官房「個人情報保護制度の見直しに関するタスクフォース」
参照 URL：https://www.cas.go.jp/jp/seisaku/kojinjyoho_hogo/

- 個人情報の保護に関する法律等の一部を改正する法律（2020 年 6 月 12 日公布）
- 個人情報の保護に関する法律についてのガイドライン（通則編、第三者提供時の確認・記録義務編、匿名加工情報編）
- 金融分野における個人情報保護に関するガイドライン
- 認定個人情報保護団体が定める個人情報保護指針[26]

② 公的分野に関するもの

- 行政機関の保有する個人情報の保護に関する法律（平成 15 年 5 月 30 日法律 58 号）
- 独立行政法人等の保有する個人情報の保護に関する法律（平成 15 年 5 月 30 日法律第 59 号）
- 地方公共団体の個人情報保護条例
- 行政機関の保有する個人情報の保護に関する法律についてのガイドライン（行政機関非識別加工情報編）
- 独立行政法人等の保有する個人情報の保護に関する法律についてのガイドライン（独立行政法人等非識別加工情報編）

3.2.2 本書での対応

本書では、前項に挙げたものの中で、行政規制としてより一般的である民間分野における個人情報保護法を前提に整理しているが、個人情報を取扱う各関連事業者は自らの組織形態に関連する行政規制に従う必要がある。

3.3 民事ルール（契約法）

3.3.1 データ利活用に関連する主な論点

個人情報の取扱いにおける契約に際し、個人情報保護法等の行政規制を遵守することは当然ながら、プライバシー権を含む人格権、または人格的利益についても配慮することが求められる。現状では、民法上、個人情報に関する規律を直接含む条項が存在しないため、プライバシー権を含む人格権、または人格的利益の侵害は、民法の一般的ルールである不法行為（民法 709 条）の枠組みで処理されている。もっとも、当該枠組み

[26] 認定個人情報保護団体は、業界・事業分野ごとの民間による個人情報の保護の推進を図るために、自主的な取組みを行うことを目的として、個人情報保護委員会の認定を受けた法人（法人でない団体で代表者又は管理人の定めのあるものを含む。）である。認定個人情報保護団体は、対象事業者の個人情報等の適正な取扱いの確保を目的として、業界の特性に応じた自主的なルールである「個人情報保護指針」を作成している。参照 URL：https://www.ppc.go.jp/personalinfo/nintei/summary/#info

は、詳細を定めるものではないため、プライバシー権を含む人格権、または人格的利益への配慮は原則として利害関係者間の契約を通じて図られることになる。

しかし、一般社団法人データ流通推進協議会が公開するパーソナルデータリファレンスアーキテクチャ[27]でも述べられている通り、プライバシー権を含む人格権又は人格的利益について処理する契約を、「専門家抜きに作成することはほとんど不可能」であり、「人格権又は人格的利益の処理などは、（中略）民法の中でも、典型契約に直ちに当てはまるものでなく、更に、条文のない分野を把握していなければ作成できないもの」である。従って、事業内容の策定、当該内容に基づく関連事業者間での契約締結及び個人情報提供者本人からの同意取得においては、個人情報保護法令の遵守にとどまらず、本人のプライバシー等についても十分に考慮した内容・手法となるように、専門家の意見も踏まえて慎重に検討しなければならない[28]。

3.3.2 本書での対応

本書では、「4.8 個人情報保護法観点で遵守すべきこと」にてプライバシーポリシーを定める際に個人情報保護法の関連条項を考慮することを提示するだけでなく、「4.5 生活支援モデルの例」「4.6 観光支援モデルの例」「4.7 交通支援モデルの例」にて、当該モデル事業を例に、ユースケースシナリオテンプレートを用いて関連事業者間の契約関係を明確にし、個人データ提供者本人からの同意取得のタイミングや取得方法について契約上整理する手法を提示する。本手法を活用することにより、利害関係者間の契約において、個人データの本人への配慮を個人情報保護法遵守の観点だけでなく、契約遵守の観点からも担保することを期待する。尚、今回のモデル事業では、個人データ提供者から取得した事業者が他のステークホルダに受け渡すときは、共同利用での受け渡しおよび、統計情報を受け渡したこともあり、個人情報保護法の範囲に留まる対応となった。今後第三者提供を実施する際には、個人データの本人の人格権、または人格的利益についても配慮がなされるよう努めたい。

---

[27] 一般社団法人データ流通推進協議会（DTA）公表（公表日：令和 2 年 3 月）
リファレンスアーキテクチャ書
参照 URL：https://data-trading.org/wp-content/uploads/2020/06/02_PersonalDataReferenceArchitecture_DesignDocument_FirstEd.pdf
リファレンスアーキテクチャ書（設計書）の概要書
http://data-trading.org/wp-content/uploads/2020/06/01_PersonalDataReferenceArchitecture_Overview_FirstEd.pdf

[28] データ利用の契約に関する具体的な手法については、経済産業省「AI・データの利用に関する契約ガイドライン（データ編）」（令和元年 12 月公表）を参考にされたい
参照 URL：https://www.meti.go.jp/press/2019/12/20191209001/20191209001-2.pdf

4 活用編

本章では、データを取扱う事業全体を俯瞰して、データの取扱いの適正性を確認し、潜在する課題を顕在化させることができるように、データ利活用基盤の構築を検討する際の共通手法について説明する。

4.1 活用編の位置づけ

本章で記載した手法は、「図表 4　データ利活用におけるロールと想定される各関連事業者」で示した、データ利活用推進主体、データ利活用基盤システム運用者、データ分析者にあたる各関連事業者（以下、データ利活用推進主体等という）が、適切なデータの利活用基盤を構築できるように整理したものである。また、その手法を用いて今回のモデル事業について検証する。

データ利活用推進主体等が課題を見据え、その解決方針を定めた後、実際にデータを取扱う事業全体を俯瞰して検討する際には、様々な観点で検討の漏れの無いように進める必要がある。モデル事業の検証を進める際にも、3 つのモデル事業間の比較ができるよう共通の手法で表現し、検証を進めることが望ましい。

本書では、内閣府「戦略的イノベーション創造プログラム（SIP）第 2 期／ビッグデータ・AI を活用したサイバー空間基盤技術／パーソナルデータアーキテクチャ構築」事業で作成され、一般社団法人データ流通推進協議会が公開するパーソナルデータリファレンスアーキテクチャのユースケースシナリオテンプレートを共通の手法として用いる。

パーソナルデータリファレンスアーキテクチャでは、「パーソナルデータ」を「個人に関するデータ、つまり個人情報保護法に規定する個人情報に限らず、かつ個人識別性の有無に拘らず、位置情報や購買履歴等広く個人に関する情報を構成しうるデータ」と定義している。決済データや購買データも「パーソナルデータ」に含まれるものであり、それらデータの取扱い方法を検討する際にもパーソナルデータリファレンスアーキテクチャのユースケースシナリオテンプレートは適切なものである。

ユースケースシナリオテンプレートでは、ステークホルダリスト、ビジネス関係図、データリソースマップ、トラストリソースマップ、データフローシーケンス、法制関係表の 6 つのテンプレートを提供しており、次節以降にて利用手順を説明する。

4.2 ユースケースシナリオテンプレートの利用手順

ユースケースシナリオテンプレートの利用手順は次の通りである。各テンプレートを作成する際に相互に影響を与える場合は、都度必要なテンプレートの修正を行うため前の手順に戻ることもある。

図表 8　ユースケースシナリオテンプレートの利用手順

No	テンプレート	作成手順
(1)	ステークホルダリスト	データ利活用に関わる存在(エンティティ)を洗い出す。人、組織含め漏れなくリストアップする。
(2)	ビジネス関係図	ステークホルダリストに記載されているステークホルダ間のビジネス関係(事業者間の契約や同意の取得、物販や役務等)を明記する。
(3)	データリソースマップ	ビジネス関係図と重なるような形で、どの存在(エンティティ)で、どのようなデータを持っているのかを整理する。またステークホルダ間でのデータ授受内容についても明確にする。
(4)	トラストリソースマップ	ステークホルダ間の認証の有無、認証方法を整理する。
(5)	データフローシーケンス	モデル事業で必要となるデータ授受に関して、時系列に記載する。記載に当たってはビジネス関係図、トラストリソースマップ等を参照し、整合性を確認する。
(6)	法制関係表	ステークホルダ間の遵守事項と、その拠りどころを明確にする。拠りどころは個別の契約による場合もあれば、法制に基づくものもある。

4.3 ユースケースシナリオテンプレートの記載方法

本節では、ユースケースシナリオテンプレートの具体的な記載方法について、パーソナルデータリファレンスアーキテクチャ書（設計書）の中で記載例として取扱われているドライブレコーダの例[29]を用いて説明する。

4.3.1 ステークホルダリスト

ステークホルダリストを作成する目的は、データが取扱われる範囲を明確にすることで事業に係わるステークホルダに抜けが無いようにすることや、各ステークホルダリストの個人情報保護法制における位置づけを明確にすることである。

[29] パーソナルリファレンスアーキテクチャ書（設計書）　9.3.2 記載例(P92-101)
参照 URL：https://data-trading.org/wp-content/uploads/2020/06/02_PersonalDataReferenceArchitecture_DesignDocument_FirstEd.pdf

あるステークホルダの取扱うデータが個人情報に該当する場合は、ステークホルダリストに個人情報取扱事業者に該当することを記載する。これにより事業に関わるステークホルダと個人情報との関係性を明確にすることができる。

図表 9　ステークホルダリスト（例）

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール名
ドライバ	無	ドライブレコーダで録画した映像を提供	データ提供者
ドライブレコーダ販売事業者	無	ドライブレコーダを販売	※1
データ蓄積事業者	有	ドライバから提供された映像を蓄積管理する。映像加工（非個人情報化）をデータ加工事業者へ委託する。映像を購入したい事業者へ販売する。個人情報保護法上の個人情報取扱事業者に該当	データ利活用推進主体
データ加工事業者	有	データ蓄積事業者から映像加工（非個人情報化）を受託する個人情報保護法上の委託先に該当	データ利活用基盤システム運用者
データ購入事業者	無	データ蓄積事業者から映像を購入	データ利活用者
通行人 ※2	無	ドライブレコーダが録画した映像に映り込んでいる人	

ステークホルダリスト記載時の留意点

注釈	説明
※1	ドライブレコーダ販売事業者は、どのようなロールに該当する可能性があるかを記載に当たって検討する。ここでは、映像を記録するドライブレコーダを販売した者として関与しているが、ドライブレコーダ販売事業者が提供するデータが無いことを確認し、ロールの定義を不要と判断する。
※2	データ蓄積事業者が販売する録画された映像に、通行人が映り込んでいることから、ステークホルダとして通行人も含める。 尚、通行人は個人情報を提供する意志がないことから、データ提供者にはなりえない。

4.3.2　ビジネス関係図

ビジネス関係図を作成する目的は、ステークホルダリストに示されたステークホルダ間のビジネス関係（契約等）を明確にすることである。

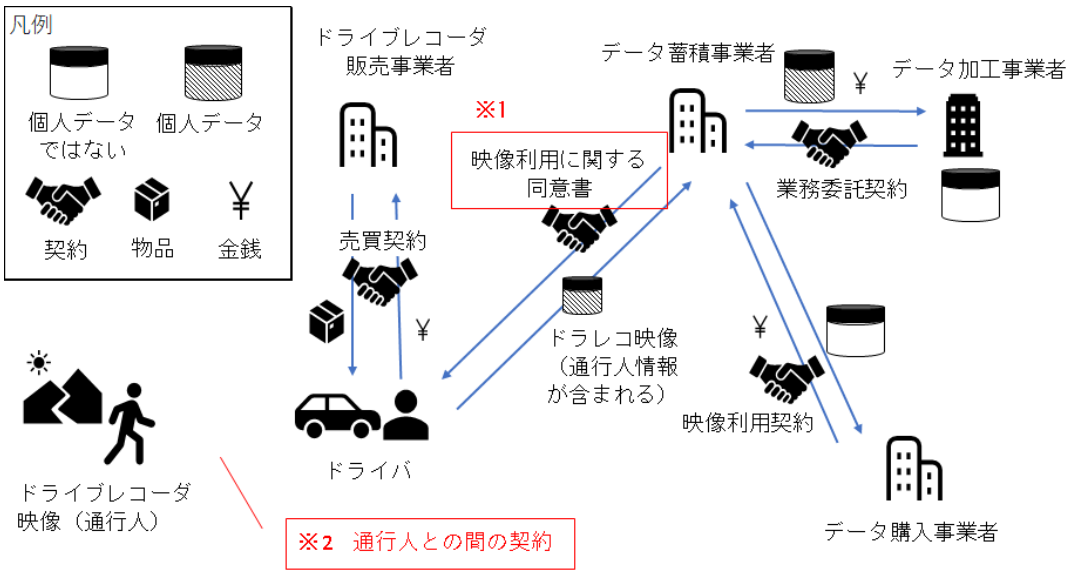
ビジネス関係図には、まずステークホルダリストに記載されたステークホルダを配置し、ステークホルダ間の契約・データの流れ・物販や役務の提供等を、アイコンと矢

印により記載する。この時、アイコンだけでなくその詳細を示す簡単なタグ名を付し、契約の形態等についても表記する。

事業者間においては、契約に基づいて他者にデータの処理や利用を委任する準委任契約のような形態や、純粋に他社にデータの提供を行う場合の契約等が存在する。どのステークホルダがどのデータを取扱い、責任を負うのかを明確にするためには、契約形態が明示される必要がある。

また、各ステークホルダの間では、契約に基づきデータ以外にも物品や役務の提供が行われ、このような行為に起因したデータが生成される場合もある。さらには、このような特定の個別契約を有しない、サービス提供や物販等に起因してデータが生成されている。これらの生成されたデータについてもビジネス関係図に明示することにより抜け漏れの無い検討が可能になる。

図表 10　ビジネス関係図（例）



ビジネス関係図記載時の留意点

注釈	説明
※1	ドライバは、自己の保有するドライブレコーダの画像をデータ蓄積事業者に提供しているが、この時の契約内容について誰がどのような責任を持つのか明確にする必要がある。
※2	ステークホルダの一つである通行人は、他のステークホルダとの間で契約関係が存在しない。しかし、ドライバはドライブレコーダの映像を第三者に提供しているので、その旨を通行人他に対して通知する必要があるのではないかという検討事項が浮かび上がる。ドライバ自身が通行人に個別に通知することは難しく、※1 で示した契約内容にも影響することがわかる。

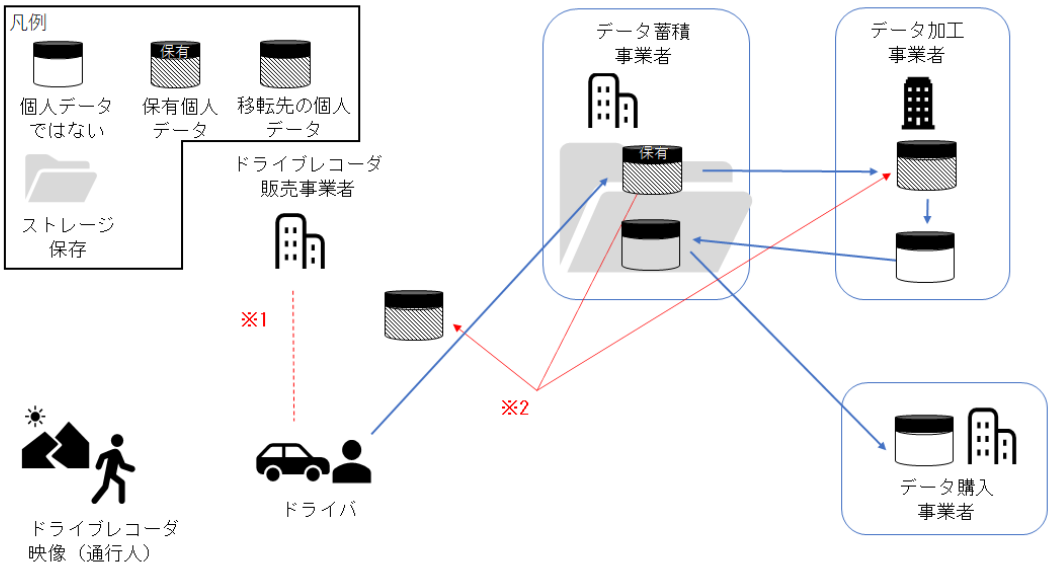
4.3.3 データリソースマップ

データリソースマップを作成する目的は、個人に関するデータがどこに存在するかを明確にすることである。

データリソースマップには、まずステークホルダリストに記載されたステークホルダを配置し、そのステークホルダ間にて移動、存在するデータの種類や移動、加工処理を、アイコンと矢印により記載する。データの存在をアイコンで示し、そのデータが個人データ、個人データを仮名加工したもの、匿名加工したもの、若しくは統計化（非個人情報化）したもの、いずれに該当するかを区別できるように記載する。また個人データの保有者を区別することにより、データ提供者から個人データの削除依頼があった場合に、どのステーホルダの責任で対応すべきかを示すことができる。尚、ステークホルダの配置は、ビジネス関係図と同じものを用いることにより記載漏れを防ぐことができる。アイコンだけではなく、必要に応じて詳細を示す簡単なタグ名を付し、データ加工の形態等も表現する。

データリソースマップを用いることにより、事業遂行する上でのセキュリティを確保すべき箇所や、インシデント発生時の影響範囲、事業譲渡や事業終了等に伴う処理範囲を明確に把握することが可能となる。

図表 11　データリソースマップ（例）



データリソースマップ記載時の留意点

注釈	説明
※1	ドライブレコーダ販売事業者は、ステークホルダリストに記載されており、ビジネス関係図では、ドライバとの物品の売買契約を行っている。しかしながら、データリソースマップには、データの取扱いが示されていない。ドライブレコーダ販売事業者の保持しているデータに個人情報と紐づくリスクがないのかをこの機会に確認すべきである。
※2	個人データがどこにあるのかを明確にする。これにより、ステークホルダ間においてどのステークホルダが何をするべきかを可視化することができる。

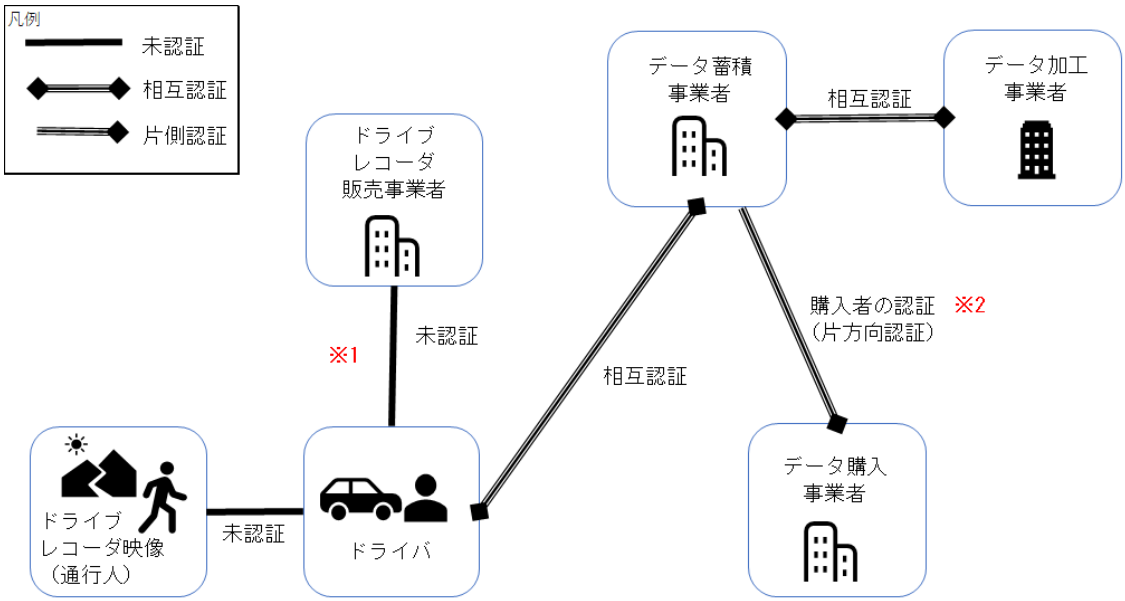
4.3.4 トラストリソースマップ

トラストリソースマップを作成する目的は、各ステークホルダ間でのトラスト関係を明確にすることである。

トラストには、二つの意味が存在する。一つ目はステークホルダに対するトラスト、もう一つは取扱われるデータに対するトラストである。ステークホルダに対するトラストとは、各ステークホルダが関連するステークホルダの認証をどのように行っているかを指す。

トラストリソースマップでは、どのような認証や確認が行われているかを明確にすることが重要である。作成にあたり、まずステークホルダリストに記載されたステークホルダを配置し、そのステークホルダ間での認証や確認の有無をアイコンと矢印により記載する。なお、ステークホルダの配置は、ビジネス関係図と同じものを用いることにより記載漏れを防ぐことができる。アイコンだけでなく、必要に応じて詳細を示す簡単なタグ名を付し、認証の形態等も表現する。

図表 12　トラストリソースマップ（例）



トラストリソースマップ記載時の留意点

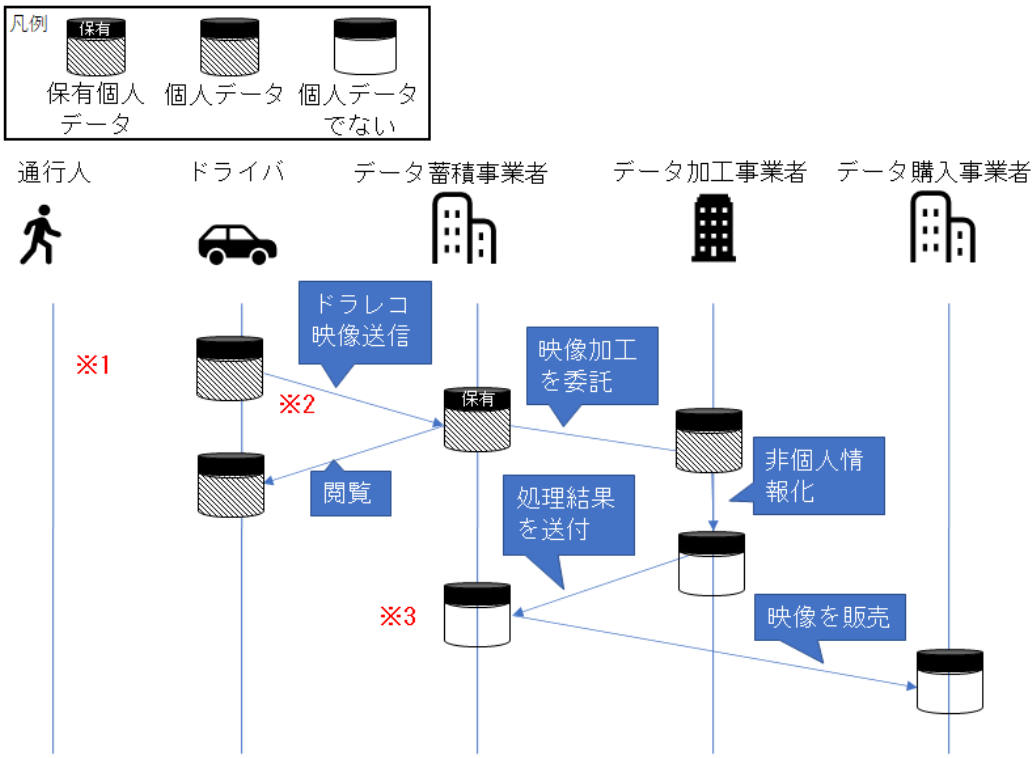
注釈	説明
※1	ビジネス関係図では、ドライブレコーダ販売事業者はドライバと売買契約を行っている。しかしながら、上記のトラストリソースマップでは、未認証であることを示す。これは、その売買契約において契約当事者の確認が行われていない可能性を示唆している。 これにより、売買契約等における未認証が許容可能なリスクであるか、検討する必要性を認識できる。
※2	データ購入事業者は、データ蓄積事業者を認証してない。この機会に許容可能なリスクであるかを検討できる。

4.3.5 データフローシーケンス

データフローシーケンスを作成する目的は、記載されるユースケースで利用されるデータについて、その発生、又は作成された時点からユースケース上で想定されるサービスが完了する時点までのデータの遷移や遷移に対する制御の手順を、時系列に沿って明確にすることである。

データフローシーケンスは、まずステークホルダリストに記載されたステークホルダを横方向に配置し、そのステークホルダ間でのデータの授受を時系列に縦方向に、アイコンと矢印により記載する。記載にあたっては、アイコンだけでなく必要に応じて詳細を示す簡単なタグ名を付し、手順上取り交わされる情報や ID の形態等も表現する。

図表 13　データフローシーケンス（例）



データフローシーケンス記載時の留意点

注釈	説明
※1	データフローシーケンスでは、ドライバと通行人の間には、情報のやりとりが存在しないことがわかる。しかしながら、プライバシー原則に照らして考えると、ドライバはドラレコ映像を第三者に提供しているので、その旨を通行人他に対して通知する必要が浮かび上がる。従って、この機会に通行人他に対する通知の実現可能性もしくはその代替策について検討する。
※2	データフローシーケンスでは、ドライバが当該サービスの停止や解約を行う場合、提供済みデータの抹消等の手順が、記載時点では明確になっていないことが判る。この機会に検討の足りていないシーケンスの有無を再確認する。
※3	データフローシーケンスでは、ドライバがデータ蓄積事業者に対してドライブレコーダの映像を提供しているが、データ蓄積事業者がデータ加工事業者やデータ購入事業者へデータを提供する際には、なんら通知等が無いことがわかる。この事は、ドライバから提供以後の全てのデータ取扱いに個別・逐次の関与がなく、包括的なデータ提供がなされていることを示している。契約におけるデータの取扱いについての妥当性を確認する。

4.3.6 法制関係表

法制関係表を作成する目的は、ステークホルダ間に存在する契約や遵守すべき法制を明確にすることにある。個人情報を取扱う事業では、個人情報保護法（第 23 条 1 項第三者提供）、業務委託契約、独立行政法人等の保有する個人情報の保護に関する法律等と、個別の事業に関する業法と並行して考慮すべき情報法制が多数存在するため、これらをリストアップすることで、留意すべき法制を明確にする。法制関係表は、ステークホルダを縦、横に配置したマトリックスを作成し、その交点に関係する法制や契約をマッピングすることで、網羅性を確認する。なお、マッピングに際しては前述の様に参照して考慮すべきものが多数あるため、弁護士等の専門家に相談の上作成することが望ましい。

図表 14　法制関連表（例）

	ドライバ	ドライブレコーダ販売事業者	データ蓄積事業者	データ加工事業者	データ購入事業者	通行人
ドライバ	NA	販売契約	映像に関する同意 個人情報保護法 ※1			
ドライブレコーダ販売事業者	販売契約	NA				
データ蓄積事業者	映像に関する同意 個人情報保護法		NA	業務委託契約 個人情報保護法	映像利用契約	個人情報保護法 ※2
データ加工事業者			業務委託契約 個人情報保護法	NA		
データ購入事業者			映像利用契約		NA	
通行人			個人情報保護法			NA

法制関係表記載時の留意点

注釈	説明
※1	ドライバとデータ蓄積事業者との間には映像利用に関する同意書が存在し、そこには、二次利用（データの加工・販売）の旨の記載が必須であることがわかる。
※2	通行人とデータ蓄積事業者との間には、個人情報保護法に関わる可能性があることがわかる。対応策を弁護士等の専門家を交えて検討する契機となりうる。

4.4 ユースケースシナリオテンプレートの活用事例

総務省「地域における決済情報等の利活用に係る調査」において、データ利活用のモデル事業を 3 地域で実施した。モデル事業は地域ウォレットで QR コード決済のデータ等を取得しデータ利活用に利用した。次節に続く「0

生活支援モデルの例」「4.6 観光支援モデルの例」「4.7 交通支援モデルの例」にて、当該モデル事業においてユースケースシナリオテンプレートを用いたデータの取扱いや契約関係の整理を記載するとともに、各モデル事業の設計、及び実施結果において今後の参考となるポイントや留意点等について記載する。尚、当該活用事例は、総務省「地域における決済情報等の利活用に係る調査」にて実施したモデル事業に基づいて記載を行っているが、当該モデル事業の設計内容、実施の詳細、モデル事業参加企業、決済事業者、及び使用技術等は、汎用性の観点から具体名を排し、実運用を見据えた時に想定される企業・団体に置き換えて記載する。

総務省「地域における決済情報等の利活用に係る調査」におけるデータ利活用のモデル事業では、決済データ等を地域で利活用する場面を仮説的に設定し、地域の課題とデータ利活用方法、目指す姿を次のように設定した。

図表 15　データ利活用方法と目指す姿

		生活支援（和歌山）	観光支援（埼玉）	交通支援（福島）
地域の課題（仮説）		• 今後深刻化が明白な買い物弱者課題に対策を具体化できていない • 潜在的な買い物弱者候補を見える化し、各種対策案の実現可能性を早期に検討する必要がある	• 観光資源に訪れた人に周辺店舗に立ち寄って頂き地域活性化につなげたい • 観光資源に訪れた人の周辺経済への効果が把握できていなく、また呼び込むための仕掛けも持っていない	• 地域交通の持続可能性の観点より、自家用車以外の地域の交通手段を強化する必要がある • 相乗りタクシー等スモールスタートできる交通手段でビジネス化成立の可能性を測りたい
データ利活用方法	対象データ	利用者個人毎に紐づけられたデータ 1. 買い物車両の乗車情報 2. 小売店舗（スーパー）での購買の決済データ及びPOSからの購買明細 3. 各種解決策への要望を問うアンケートデータ	利用者個人毎に紐づけられたデータ 1. 観光資源での決済情報 2. 周辺店舗への決済情報を含む立ち寄り情報 3. 観光客の利用者属性情報 4. 周辺店舗の属性情報	利用者個人毎に紐づけられたデータ 1. 相乗りタクシー（交通手段）での決済情報・行先情報 2. 相乗りタクシーに乗る前の長距離バスの情報 3. 長距離バス発着地近辺での決済情報（券売所・売店等）
	データ取得方法	地域のウォレットアプリにてQR決済、買い物バスチケット、個人属性情報を一元的に取得する。モデル事業後アンケートは、アプリを用いず取得する	地域のウォレットアプリにてQR決済、来店情報、個人属性情報を取得し、周辺店舗マッチングを一元的に取得する	地域のウォレットアプリにてQR決済、タクシー配車情報、クーポン利用情報、長距離バスの情報、店舗での決済情報等を一元的に取得する
目指す姿（課題解決後）		①潜在的な買い物弱者を特定できる ②買い物弱者候補の各種解決策への要望を把握できる ③買い物弱者候補の購買傾向の情報より、各種解決策実施を具体的に検討することができる	①観光資源に訪れた人の周辺店舗への立ち寄りの動態が把握できる。今後の観光資源の強化や周辺店舗の増強など、活性化に向けての打ち手がみえる ②周辺店舗の属性情報を地域で充実させ、来店予測の精度を向上する仕掛けを地域として持つことができる	①相乗りタクシーの利用促進に決済情報が貢献できるかを検証 ②相乗りタクシーにおける配車最適化に決済情報が貢献できるかを検証 ③相乗りタクシーの用途分析に本モデル事業のアウトプットデータが貢献できるかを検証

4.5 生活支援モデルの例

4.5.1 生活支援モデルの概要

生活支援モデルでは、和歌山県にて買い物弱者課題解決のためのデータ利活用事業を実施した。実施したモデル事業を基にユースケースシナリオテンプレートを記載しているが、一部事務局が担当したロール等は抽象化し、実運用を見据えた時に想定される企業・団体に置き換えて記載する。

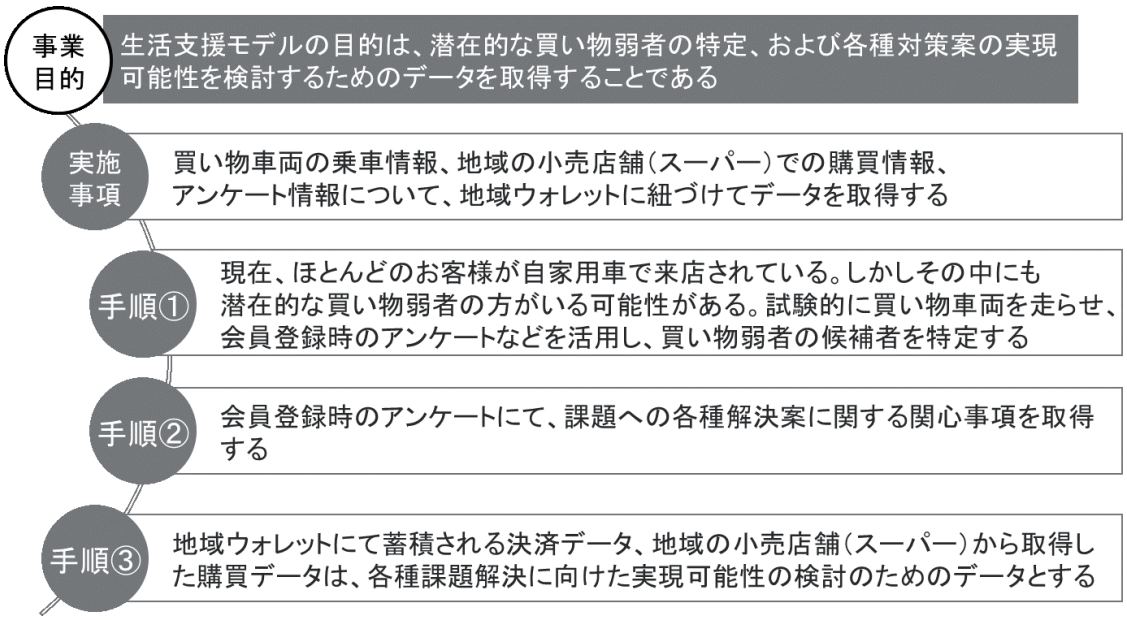
① 地域課題

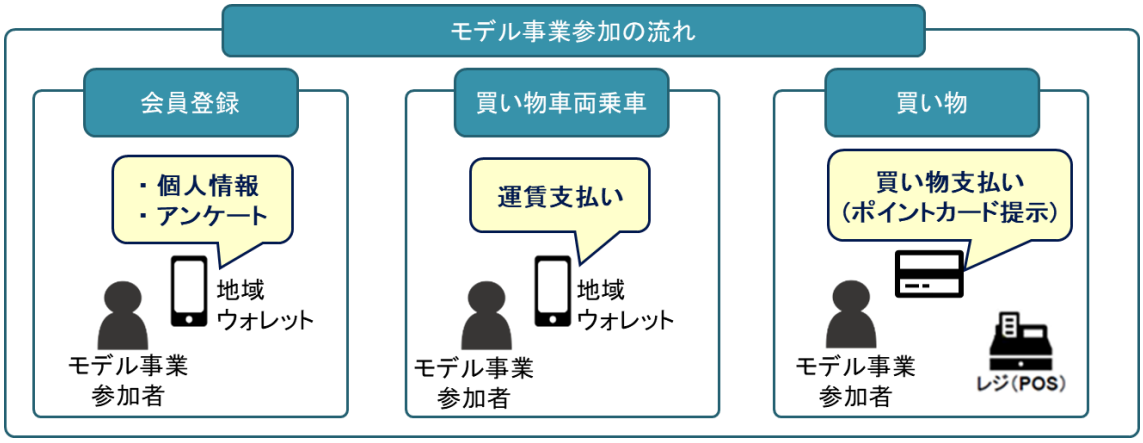
- 今後深刻化が明白な買い物弱者課題に対策を具体化できていない
- 潜在的な買い物弱者候補を見える化し、各種対策案の実現可能性を早期に検討する必要がある

② 実施事項

買い物車両の乗車情報、地域の小売店舗（スーパー）での購買情報、個人へのアンケート情報のデータを収集・突合し、買い物弱者対策の検討を実施する

図表 16 概要説明（生活支援モデル）





モデル事業参加者は、スマートフォンアプリ（地域ウォレット）から事前に会員登録を行う。その上で買い物車両に乗車し、運賃支払いの際に、地域ウォレットアプリを利用し決済する。その後、モデル事業参加者は地域の小売店舗（スーパー）で買い物をし、代金を支払う際に地域の小売店舗（スーパー）のポイントカードを提示する。地域ウォレットは、モデル事業参加者の買い物車両の乗車情報、地域の小売店舗（スーパー）での購買情報及び、アプリの会員登録時にモデル事業参加者が入力するアンケート情報を地域ウォレット ID に紐付けてデータを取得する。

4.5.2 ステークホルダリスト（生活支援モデル）

図表 17　ステークホルダリスト（生活支援モデル）

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール名	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
自治体の外郭団体[30]等	有	買い物弱者課題を解決したいと考えている主体者。 地域ウォレット及びデータ利活用基盤のオーナー。 モデル事業参加者情報、地域ウォレットを通して取得される決済入力データの保有者。 仮名加工したデータをシステム開発会社等から取得し、買い物弱者に対する課題の検討を行う。 決済事業者と包括加盟店契約を締結し加盟店開拓、管理を実施。 共同利用における個人データ管理の責任者。	データ利活用推進主体・データ利活用基盤システム運用者	地域ウォレット事業者
システム開発会社[31]等	有	地元のシステム開発会社等。自治体の外郭団体等からデータ利活用基盤の運用を受託。（個人情報保護法上の委託先に該当） 利用者属性データ、決済データ、購買データを突合した情報の作成者。　**ポイント 1**	委託(データ利活用基盤システム運用者)	－
データ分析会社[32]等	有	地元のデータ分析会社（ベンチャー）等。 仮名加工したデータをシステム開発会社等から取得し、買い物弱者に対する課題の検討を行う。	データ分析者	－
小売店舗等	有	地元の小売店舗、スーパー等。 モデル事業参加者が地元の小売店舗やスーパー等で買い物する際の決済情報、購買情報の保有者。 買い物時に、ポイントカードを提示した場合、決済情報、購買情報とポイントカード情報が紐づいて管理される。 今回のモデル事業においては、買い物車両乗車日時とポイントカード情報をキーに、地元の小売店舗やスーパー等での買い物情報をシステム開発会社等へ連携。	**ポイント 2** データ提供者 データ分析者	店舗
決済事業者[33]	有	決済用の API 提供者・電子決済代行業者。 地域ウォレットを通して、決済金額等をシステム開発会社等から受領し決済処理を実施。	データ提供者	決済事業者

[30] モデル事業では事務局を請け負った 3 社がデータ利活用推進主体のロールを担当した。
[31] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。
[32] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。
[33] モデル事業ではポイントサービスを使用した。

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール名	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
モデル事業参加者	無	モデル事業参加者。買い物車両に乗車し、地元の小売店舗やスーパー等で買い物する本人。	データ提供者	－
バス事業者 タクシー事業者等		地元の小売店舗やスーパー等までモデル事業参加者を運ぶ買い物車両を運営。 モデル事業参加者の本モデル事業における個人情報は保持しない。	- ポイント 3	－

① 決済情報の保有個人データ[34]

図表 18 データ利活用する項目の個人データ保有者（生活支援モデル）

	データ保有者		データ利活用の対象項目
	自治体の外郭団体	決済事業者	
地域ウォレット ID に紐付く決済金額	●	－	対象
地域ウォレット ID に紐付く決済結果	●	－	対象
地域ウォレット ID に紐付く決済日時	●	－	対象
地域ウォレット ID に紐付く決済時の位置情報	●	－	対象
地域ウォレット ID に紐付く決済店舗 ID	●	－	対象
取引情報（決済取引データ）	－	●	－
精算情報（決済取引データ）	－	●	－

ステークホルダリスト記載時の留意点（生活支援モデル）

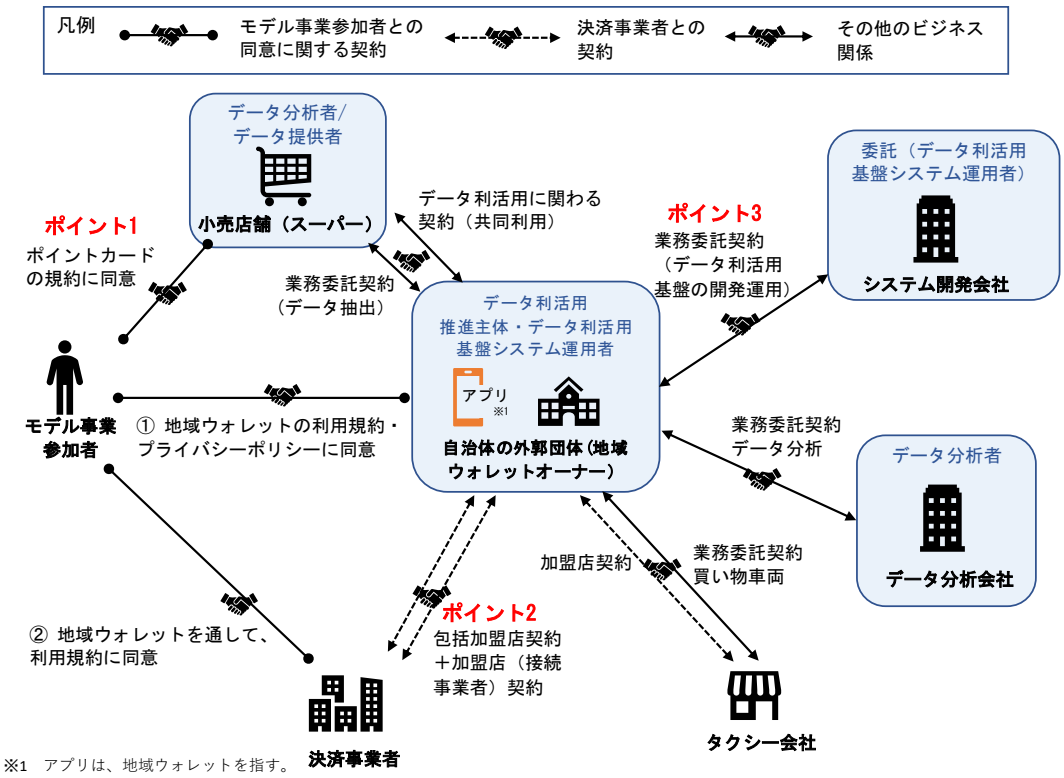
ポイント	説明
1	「決済情報」が地域ウォレットの保有個人データとなるのかを判断するため、以下 2 点を確認する。 • 決済事業者との契約 • 決済時の画面を地域ウォレットが提供していることがモデル事業参加者目線で容易に判別できること（決済事業者が提供する画面での決済の場合等においては、決済情報が地域ウォレットの保有個人データとならない可能性が高いため） 生活支援モデルでは、決済入力データは、地域ウォレット＝自治体の外郭団体等の保有個人データとなる。

[34] 保有個人データの法的な定義については、通則編（2-7 保有個人データ）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf

ポイント	説明
2	「データ提供者」を洗い出す。 データ利活用のために必要なデータを洗い出し、データを収集するための契約を締結する必要がある。
3	バス事業者タクシー事業者等は運行上で利用者の顔は認識できる。そのため、契約上業務で知りえた情報を口外しないよう契約する必要がある。（守秘義務契約）

4.5.3 ビジネス関係図（生活支援モデル）

図表 19　ビジネス関係図（生活支援モデル）



※1　アプリは、地域ウォレットを指す。

①　モデル事業参加者との契約関係

モデル事業参加者からデータ取得とデータの利用目的に関する同意を取得するタイミングは大きく二回ある。モデル事業参加者が地域ウォレットアプリの利用を進める中で、利用目的ごとの同意取得タイミングが複数存在する。

- ポイントカード利用の申込タイミング
- ウォレットアプリでの利用タイミング
  - ①　初回起動時（アカウント登録前）
  - ②　決済事業者とのサービス登録前

②　決済事業者との契約関係

システム開発会社等は、決済事業者との接続に関する契約（接続事業者となる契約）を締結し、データ利活用推進主体である自治体の外郭団体等は加盟店の開拓や管理の責務を担う包括加盟型契約を決済事業者と締結する。そのため、バス事業者やタクシー事業者との加盟店契約は、決済事業者ではなく自治体の外郭団体等が締結する。

③ 複数ステークホルダ間で個人情報を取扱う方法

自治体の外郭団体等（データ利活用推進主体）が集めたデータは、データ分析会社等（データ分析者）や、小売店舗等（データ分析者）に連携される。連携方法としては、データ分析会社等はデータ分析の委託業務の範囲で個人情報を渡しており、小売店舗等とはデータ利活用に関わる契約（共同利用）を締結している。

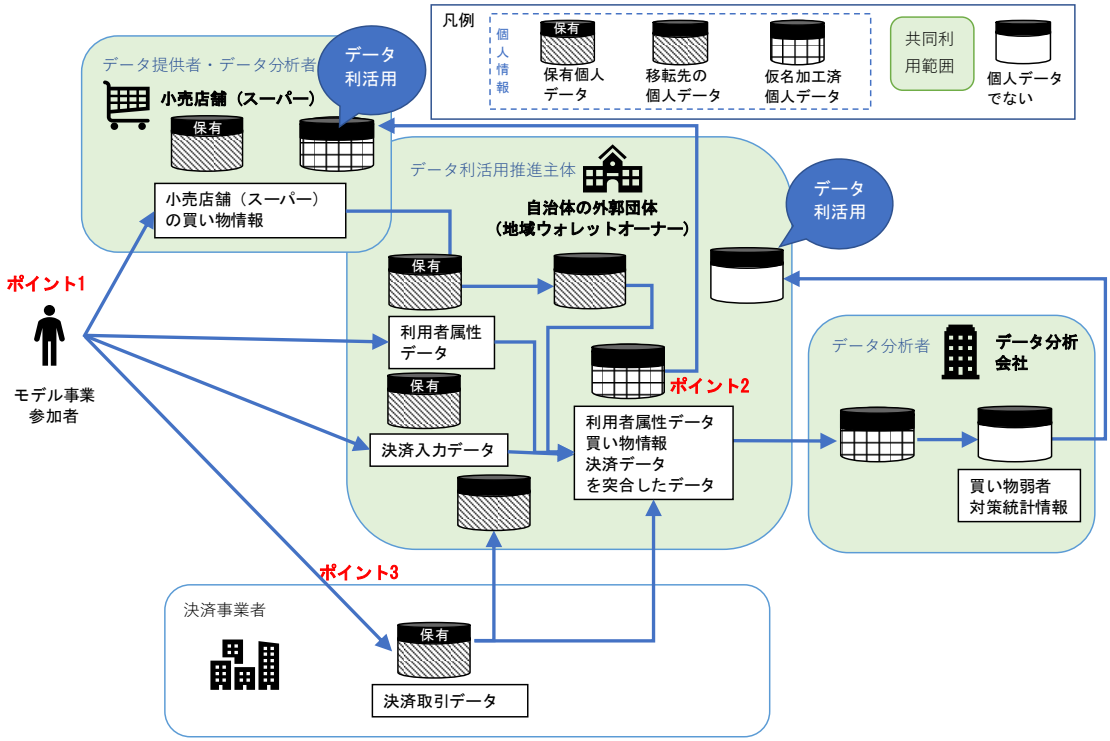
ビジネス関係図記載時の留意点（生活支援モデル）

ポイント	説明
1	モデル事業参加者から個人情報取得の同意を得る際に明示する利用目的の内容を確認する。利用目的、取得項目、第三者提供、共同利用に関する事等の記載不足がないことを確認する。 地域の小売店舗（スーパー）でのポイントカード申込時点では、利用目的に「買い物弱者対策検討のため」という記載はない。また、システム開発会社等にデータを提供すること等の記載はない。そのため、地域の小売店舗（スーパー）において直接の同意取得または地域ウォレットを経由して、ポイントカードの ID を取得するタイミングで同意を取得する。
2	決済事業者との契約を締結する上で、加盟店開拓や加盟店管理をどの主体が行うか、加盟店に関するデータをどこから入手するのか等を明確にする。
3	ステークホルダ間でのデータ連携において、モデル事業参加者のプライバシーを最大限考慮し、委託、共同利用、第三者提供のうち、適切なデータ受け渡しの法的根拠を検討する。

4.5.4 データリソースマップ（生活支援モデル）

データリソースマップを用いて、ビジネス関係図と同じ配置の状態で各ステークホルダのデータ保持と受け渡しを記載した。

図表 20　データリソースマップ（生活支援モデル）



データリソースマップ記載時の留意点（生活支援モデル）

ポイント	説明
1	モデル事業参加者から個人情報の変更依頼・削除依頼があった際は、共同利用者に連携したデータまでを変更・削除対象とする。但し、決済事業者との間で発生した取引データの削除は、関連法制に則り削除の可否が変わる。統計情報はある時点のスナップショットであるため、遡求する必要はない。
2	共同利用者間では、個人データを加工した仮名加工情報を連携しデータ分析、データ利活用する。その際、個人を特定できるマスタは共同利用者には連携しない。またデータの取扱いは個人情報同等とする。
3	決済事業者は、地域ウォレットを通して決済を実施している中で、モデル事業参加者から決済情報（決済取引データ）を取得している。

① 保持データの整理（生活支援モデル）

図表 21 自治体の外郭団体等 保持データ（生活支援モデル）

No	保有者	データの内容	データの種類
1	自治体の外郭団体等	アプリ利用者の利用者属性データ（氏名、住所、電話番号等）	個人情報・仮名加工情報
2	自治体の外郭団体等	アプリ利用者の決済入力データ（入力金額、決済店舗、決済日時等の買い物車両での決済入力データ）	個人情報・仮名加工情報
3	小売店舗等	スーパーでの買い物情報（買い物車両に乗った日の購買データ、決済データ）	個人情報・仮名加工情報
4	データ分析会社等	利用者属性データ、決済データ、買い物情報を突合しデータ分析し、統計化した情報	統計情報
5	決済事業者	決済取引データ（決済取引連番、取引情報、精算情報）	個人情報

図表 22 データ分析会社等 保持データ（生活支援モデル）

No	保有者	データの内容	データの種類
1	自治体の外郭団体等	アプリ利用者の利用者属性データ（電話番号を一意となるランダムな値に変更したもの、郵便番号、年齢等）	仮名加工情報
2	自治体の外郭団体等	アプリ利用者の決済入力データ（入力金額、決済店舗、決済日時等の買い物車両での決済入力データ）	仮名加工情報
3	小売店舗等	スーパーでの買い物情報（買い物車両に乗った日の購買データ、決済データ）	仮名加工情報
4	データ分析会社等	利用者属性データ、決済データ、買い物情報を突合しデータ分析、統計化した情報	統計情報

図表 23 決済事業者 保持データ（生活支援モデル）

No	保有者	データの内容	データの種類
1	決済事業者	決済取引データ（決済取引連番、取引情報、精算情報）	個人情報

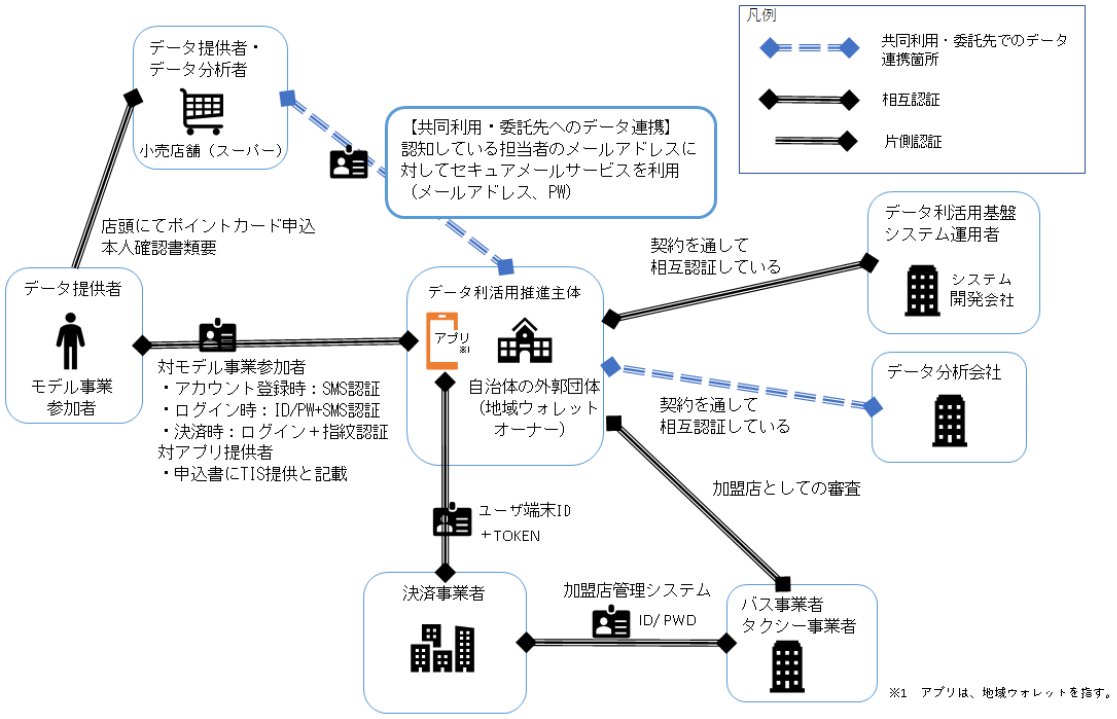
図表 24 小売店舗等 保持データ（生活支援モデル）

No	保有者	データの内容	データの種類
1	システム開発会社等	アプリ利用者の利用者属性データ（電話番号を一意となるランダムな値に変更したもの、郵便番号、年齢等）	仮名加工情報
2	システム開発会社等	アプリ利用者の決済入力データ（入力金額、決済店舗、決済日時等の買い物車両での決済入力データ）	仮名加工情報
3	小売店舗等	ポイントカード ID に紐づく買い物車両乗車日の買い物情報（決済情報、購買情報）	個人情報

4.5.5 トラストリソースマップ（生活支援モデル）

各ステークホルダ間のデータを連携する際に、どのような認証が行われているかを明確にするため、トラストリソースマップを用いて次のように整理した。

図表 25　トラストリソースマップ（生活支援モデル）



図表 26　各ステークホルダ間での認証有無（生活支援モデル）

関係 A	関係 B	A から B の認証	B から A の認証	認証
モデル事業参加者	小売店舗等	モデル事業参加者は、小売店舗等の登記簿までは確認していない。	ポイントカードの契約は、店頭申込のみ。申込時に本人確認は実施する。	片側認証
モデル事業参加者	自治体の外郭団体等等（地域ウォレット）	モデル事業参加者は市役所開催の説明会に参加し、アプリの説明を受ける。また申込書に自治体の外郭団体等のアプリであることを明記している。	SMS 認証（電話番号認証）でモデル事業参加者の本人確認を実施している。	相互認証
自治体の外郭団体等（地域ウォレット）	決済事業者	決済事業者との接続設定をする際に認証している。	口座登録時のユーザ端末 ID と、トークンを使っての認証している。	相互認証

関係 A	関係 B	A から B の認証	B から A の認証	認証
自治体の 外郭団体等	小売店舗等	お互いの信頼性は契約時に担保している。 データのやり取りについては、セキュアメールにて実施 ポイントカード ID は、地域ウォレットの氏名とセットで渡し、別人の ID が混入することを防いでいる。		相互 認証
自治体の 外郭団体等	決済事業者	お互いの信頼性は契約時に担保している。		相互 認証
自治体の 外郭団体等	システム開発会社等	お互いの信頼性は契約時に担保している。		相互 認証
自治体の 外郭団体等	バス事業者、 タクシー事業者	お互いの信頼性は契約時に担保している。		相互 認証
自治体の 外郭団体等	データ分析会社等	お互いの信頼性は契約時に担保している。 データのやり取りは、セキュアメールにて実施。		相互 認証
バス事業者 タクシー事業者	決済事業者 （加盟店管理システム）	SSL 通信でアクセスしているため、加盟店管理システムであることは認知できている。	加盟店管理システムから払いだされた ID/PW で認証している。	相互 認証

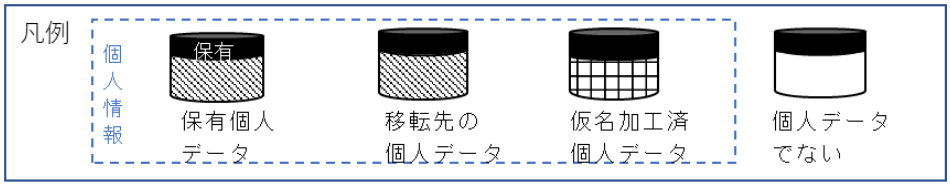
データ利活用推進主体から共同利用者・委託先へデータ共有する際の実施手順

1．決済データ・買い物情報・利用者属性データの突合データを仮名加工処理し、
　仮名加工情報とする。
2．社内での持出申請フローに従い実施する。
　－1．仮名加工情報の暗号化処理を実施する。
　－2．個人情報保護責任者に対して持出許可をもらう。
　－3．セキュアメールにて、共同利用者に対して送付する。
3．共同利用者の受信確認後、送付したデータは削除する。
4．個人情報貸し出し一覧へ記載し、破棄もしくは返却を確認してから
　クローズする。

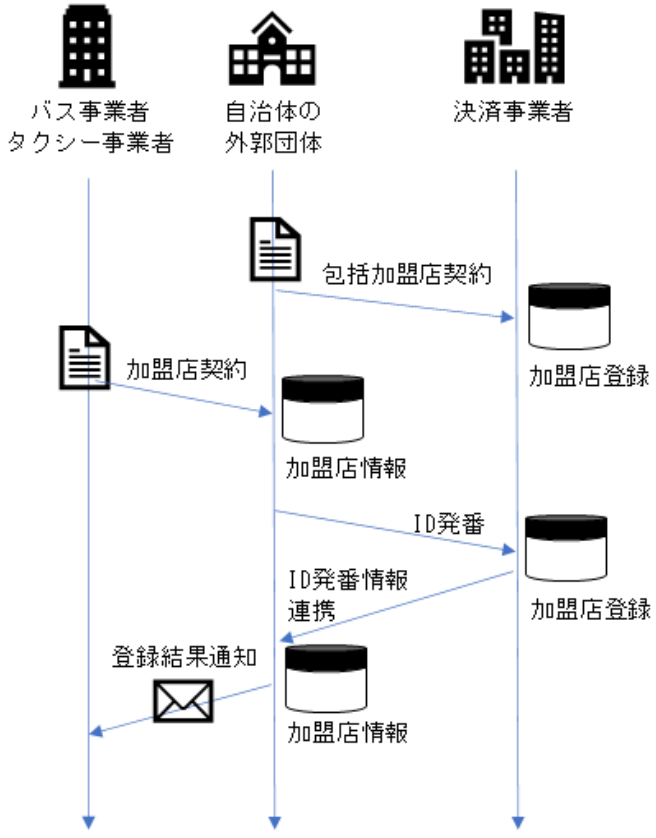
4.5.6 データフローシーケンス（生活支援モデル）

データフローシーケンスを基に、実際のモデル事業の流れを時系列にまとめる。

以下は各図表で使用するアイコンであるが、それぞれのアイコンを区別することにより、各個人データの保有者、連携先、及び加工の有無を整理する。

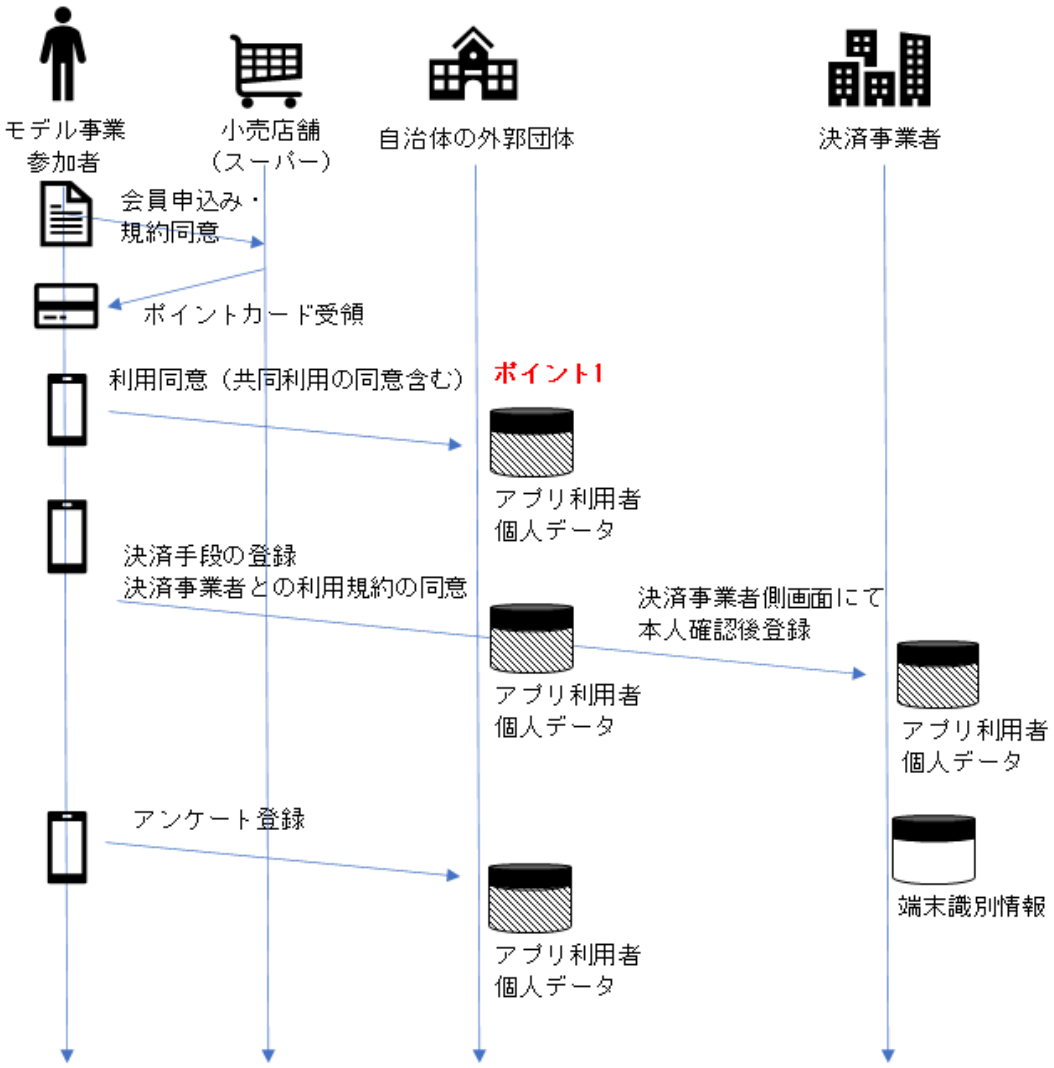


図表 27　データフローシーケンス＜加盟店契約＞（生活支援モデル）



バス事業者/タクシー事業者（加盟店）は、包括加盟店契約した自治体の外郭団体等を通して加盟店契約を締結する。

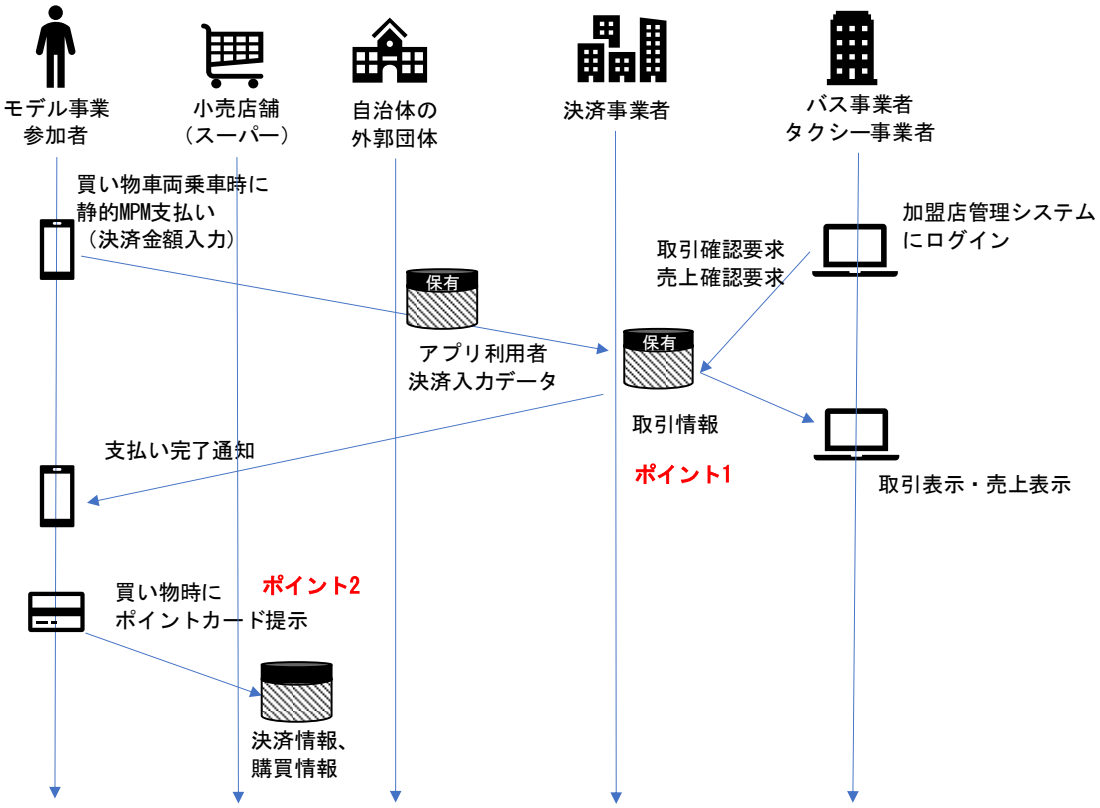
図表 28　データフローシーケンス＜会員登録＞（生活支援モデル）



データフローシーケンス＜会員登録＞の留意点（生活支援モデル）

ポイント	説明
1	個人情報の収集を始める前には、あらかじめ本人に対し利用目的の明示が必要となる。※詳細は、4.8 (2) 4「直接書面等による取得」を参照

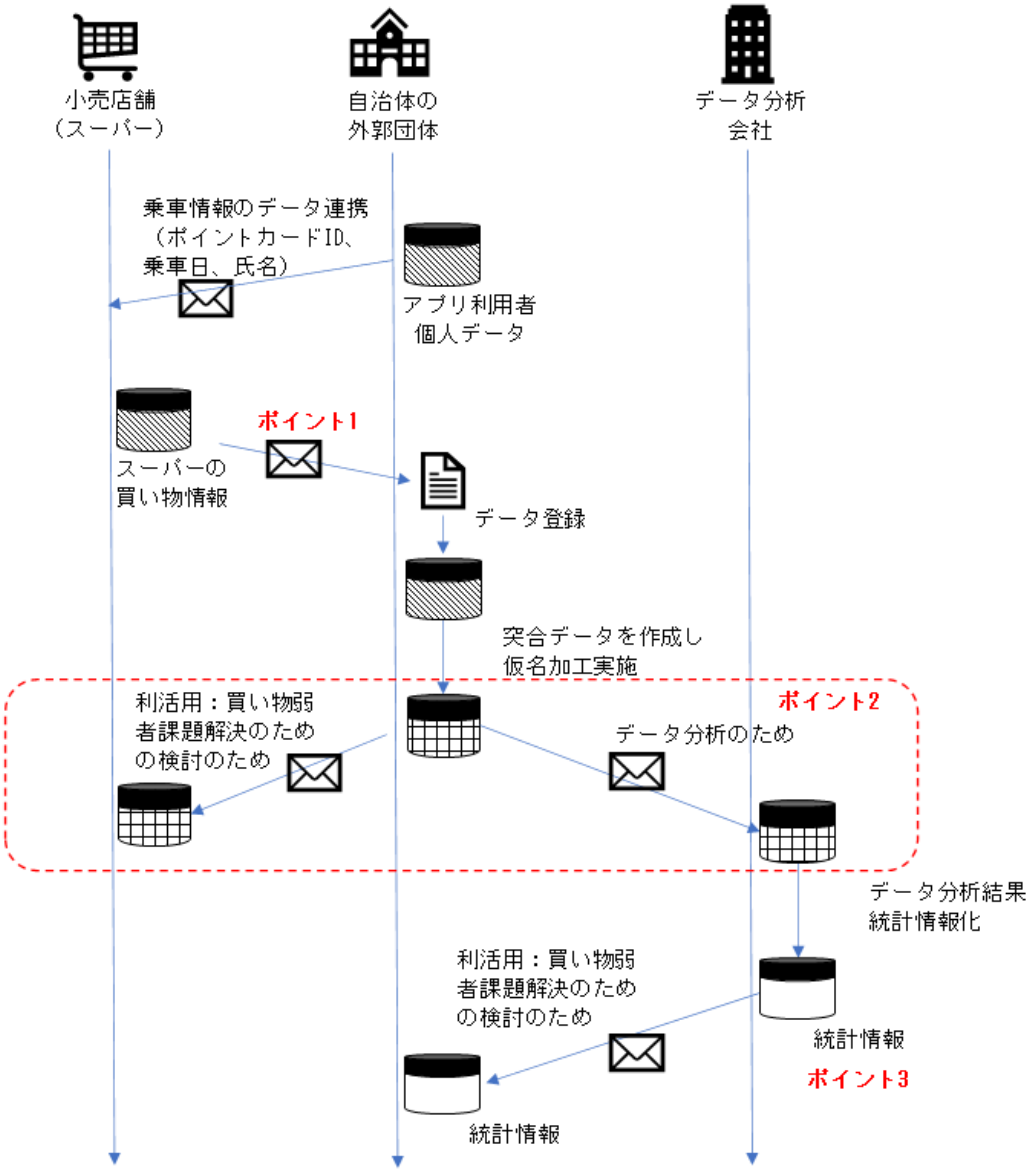
図表 29　データフローシーケンス
＜買い物バス乗車～小売店舗（スーパー）での買い物＞（生活支援モデル）



データフローシーケンス＜バス乗車～買い物＞の留意点（生活支援モデル）

ポイント	説明
1	車両乗車時の支払い情報が取引実行するために使われるため、利用目的への記載は必要となる。
2	スーパーで買い物情報とポイントカードの情報を紐づけて管理する場合個人情報に該当するため、地域ウォレットがスーパーから買い物情報を取得する際には、スーパーから本人に対し利用目的を通知・公表がなされているかを確認する必要がある。

図表 30　データフローシーケンス＜突合データ連携～分析＞（生活支援モデル）



データフローシーケンス＜突合データ連携～分析＞の留意点（生活支援モデル）

ポイント	説明
1	スーパーの買い物情報がシステム開発会社等に移転される。提供の方法によって、本人への通知等が必要。今回の場合はデータの共同利用となる。注意点は、ポイント 2 を参照されたい。
2	データ利活用するために仮名加工を実施した個人データを共同利用先に連携する。共同利用するものの範囲・共同利用者の利用目的・共同利用する個人データの項目・個人データの管理ついて責任を有するものについて本人に通知または容易に知りうる状態におく必要がある。また、仮名加工情報は本人を識別することを目的としてほかの情報と照合してはならない。 ※詳細は、4.8 (4) 4「第三者提供に該当しない場合」を参照
3	統計情報のみを利活用する場合は、その利用目的をユーザに公表等する必要はない。

4.5.7 法制関連図

各ステークホルダ間で締結する契約、及び留意すべき法律や法律で定められた制度は、次のようなものが挙げられる。ここで挙げたものが各ステークホルダ間で遵守できているか再確認する必要がある。

図表 31　法制関連図（生活支援モデル）

	モデル事業参加者	小売店舗（スーパー）	システム開発会社等	決済事業者	バス事業者 タクシー事業者	データ分析会社等	自治体の 外郭団体等
モデル事業参加者	NA	個人情報保護法（個人情報取扱事業者） 個人情報保護法（共同利用者） 会員約款同意	個人情報保護法（委託先に該当）	取引規定への同意（アプリ内で実施） 個人情報保護法（個人情報取扱事業者）	-	個人情報保護法（委託先に該当）	個人情報保護法（共同利用窓口） アプリ約款同意
小売店舗（スーパー）	個人情報保護法（個人情報取扱事業者） 個人情報保護法（共同利用者） 会員約款同意	NA	-	-	-	-	業務委託契約（データ授受） 共同利用の契約
システム開発会社等	個人情報保護法（委託先に該当）	-	NA	決済事業者との加盟契約（接続事業者） 資金決済法	-	-	個人情報取扱事業者の委託先に該当 景品表示法

	モデル事業参加者	小売店舗 （スーパー）	システム開発会社等	決済事業者	バス事業者 タクシー事業者	データ分析会社等	自治体の 外郭団体等
決済事業者	取引規定への同意 （アプリ内で実施） 個人情報保護法 （個人情報取扱事業者）	-	決済事業者との加盟契約（接続事業者） 資金決済法	NA	-	-	決済事業者との加盟契約（包括加盟型）
バス事業者 タクシー事業者	-	-	-	-	NA	-	加盟契約 バス運行の業務委託契約 道路運送法 一般乗合旅客自動車運送事業の許可
データ分析会社等	個人情報保護法 （委託先に該当）	-	-	-	-	NA	個人情報取扱事業者（委託先の監督）
自治体の 外郭団体等	個人情報保護法 （共同利用窓口） アプリ約款同意	業務委託契約 （データ授受） 共同利用の契約	個人情報取扱事業者 （委託先の監督） 景品表示法	決済事業者との加盟契約（包括加盟型）	加盟契約 バス運行の業務委託契約 道路運送法 一般乗合旅客自動車運送事業の許可	個人情報取扱事業者（委託先の監督）	NA

4.6 観光支援モデルの例

4.6.1 観光支援モデルの概要

観光支援モデルでは、埼玉県にて観光・リゾート産業の活性化問題のためのデータ利活用事業を実施した。観光資源に訪れた人の周辺店舗への立ち寄りの動態を把握し、地域の活性化につなげる。実施したモデル事業を基にユースケースシナリオテンプレートを記載しているが、一部事務局が担当したロール等は抽象化し、実運用を見据えた時に想定される企業・団体に置き換えて記載する。

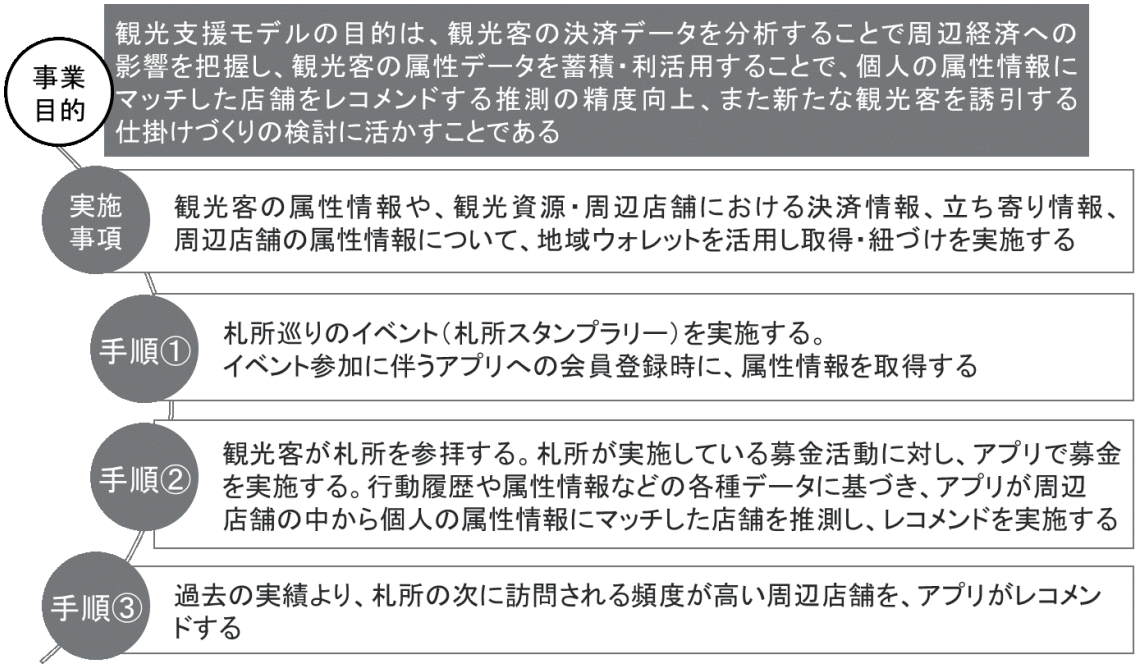
① 地域課題

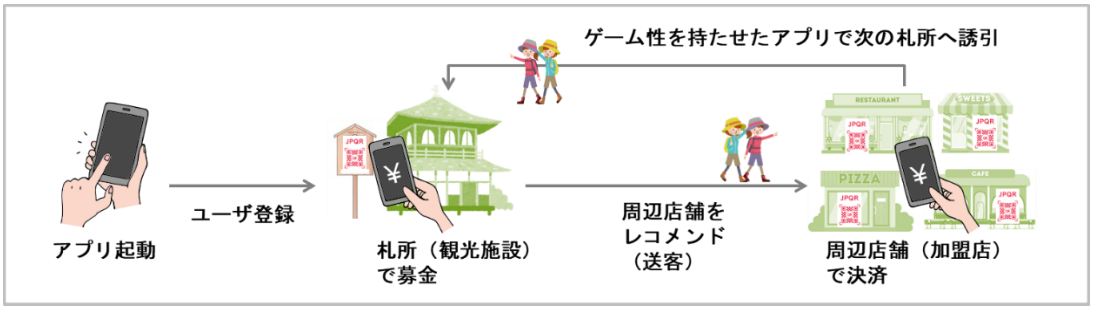
- 観光資源に訪れた人に周辺店舗に立ち寄ってもらい地域活性化につなげたい
- 観光資源に訪れた人の周辺経済への効果が把握できておらず、また呼び込むための仕掛けも持っていない

② 実施事項

観光客の決済・購買情報を分析して観光客の動態把握や予測を行い、新たな観光客の呼び込み等で地域の観光・リゾート産業の活性化に活用する。

図表 32 概要説明（観光支援モデル）





モデル事業参加者は、札所（観光資源）を訪れて募金を行う際に、スマートフォンアプリ（地域ウォレット）を利用し決済する。決済後に周辺店舗のレコメンドがアプリ上に通知される。モデル事業参加者は、レコメンドされた周辺店舗を訪れながら、アプリを使いスタンプラリーに参加する。スタンプラリーでの参加条件を満たすとプレゼント応募の権利を獲得できる。

4.6.2 ステークホルダリスト（観光支援モデル）

図表 33　ステークホルダリスト（観光支援モデル）

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
商工会議所[35]	有	地域の観光資源や周辺店舗へ観光客を誘引する等、地域活性化の課題について考えている主体者。 モデル事業協力店舗を募集し、参加店舗リストの管理を行う。 仮名加工データをシステム開発会社等から受け取る。	データ利活用推進主体	－
システム開発会社[36]等	有	ポイント 1 地元のシステム開発会社等。 地域ウォレットのオーナー。 モデル事業参加者情報、地域ウォレットを通して取得される決済入力データの保有者。 利用者属性データ、決済データ、スタンプラリーデータ、店舗リストを突合した情報の作成者。	データ利活用基盤システム運用者	地域ウォレット事業者
開発委託会社等	無	スタンプラリー機能を開発する会社。 個人情報は保有していない。		－
データ分析会社[37]等	有	地元のデータ分析会社（ベンチャー）等。 仮名加工したデータをシステム開発会社等から取得し、新たな観光客の呼び込みに活用できる分析データを作成する。	データ分析者	－
社団法人等	無	観光資源をとりまとめる一般社団法人。 スタンプラリーの対象となる観光資源（札所）の管理者		－
モデル事業協力店舗	無	観光資源に訪れた人の立ち寄り先候補。 JPQR 決済の加盟店を想定。		－
モデル事業参加者	無	スタンプラリーの参加者。札所を巡り、周辺店舗で買い物をする。主に観光客が対象	データ提供者	－
決済事業者[38]	有	決済用の API 提供者・電子決済代行業者。 店舗との間で加盟店契約を締結。 店舗（加盟店）の情報を保有。	データ提供者	決済事業者

ポイント 2

[35] モデル事業では事務局を請け負った 3 社がデータ推進主体のロールを担当した。
[36] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。
[37] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。
[38] モデル事業ではポイントサービスを使用した。

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
地方自治体	無	市民向け窓口、データ利活用結果を受け取り、地域課題の解決に活用する。	データ利活用者	－

① 決済情報の保有個人データ[39]

図表 34　データ利活用する項目の個人データ保有者について

	データ保有者		データ利活用の対象項目
	システム開発会社等	決済事業者	
地域ウォレット ID に紐付く決済金額	●	－	対象
地域ウォレット ID に紐付く決済結果	●	－	対象
地域ウォレット ID に紐付く決済日時	●	－	対象
地域ウォレット ID に紐付く決済時の位置情報	－	－	－
地域ウォレット ID に紐付く決済店舗 ID	●	－	対象
取引情報（決済取引データ）	－	●	－
精算情報（決済取引データ）	－	●	－

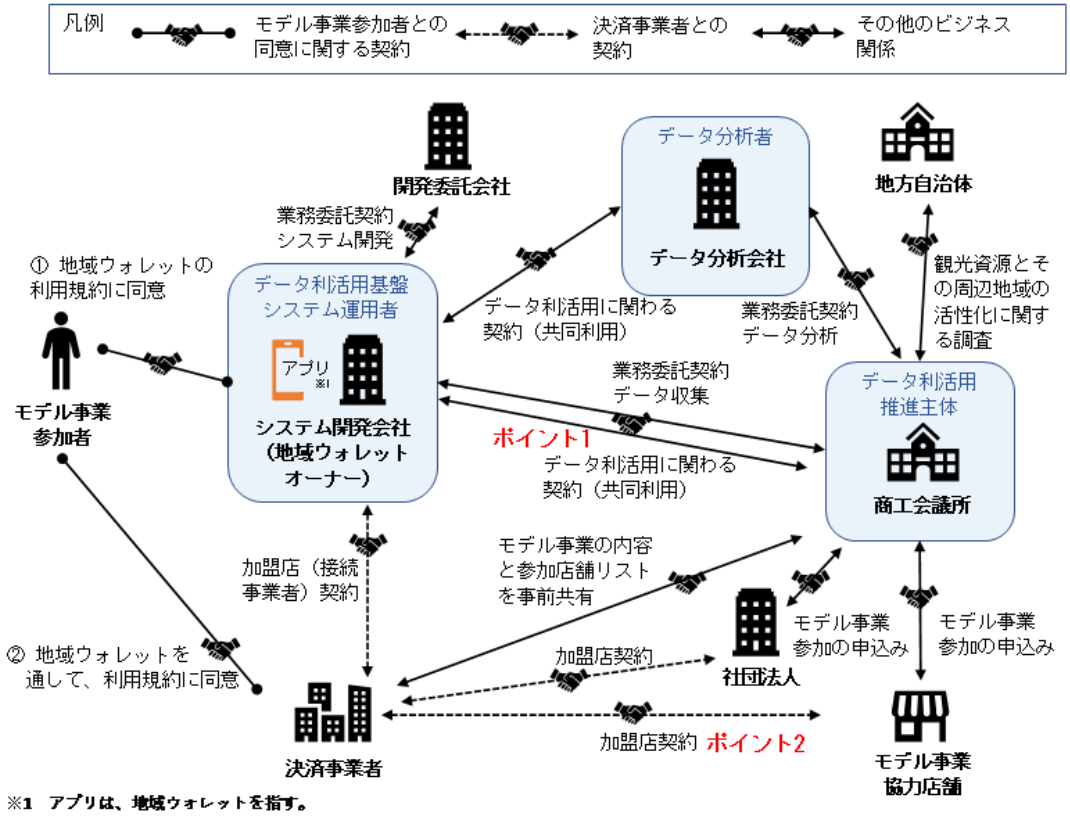
ステークホルダリスト記載時の留意点（観光支援モデル）

ポイント	説明
1	「決済情報」が地域ウォレットの保有個人データとなるのかを判断するため、以下二点を確認する。 決済事業者との契約 決済時の画面を地域ウォレットが提供していることがモデル事業参加者目線で容易に判別できること（決済事業者が提供する画面での決済の場合等においては、決済情報が地域ウォレットの保有個人データとならない可能性が高いため） 観光支援モデルでは、決済入力データは、地域ウォレット＝システム開発会社等の保有個人データとなる。
2	「データ提供者」を洗い出す。 ステークホルダ間で連携が必要なデータを洗い出し、データを収集するための契約を締結する必要がある。

[39] 保有個人データの法的な定義については、通則編（2-7 保有個人データ）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf

4.6.3 ビジネス関係図（観光支援モデル）

図表 35　ビジネス関係図（観光支援モデル）



①　モデル事業参加者との契約関係

モデル事業参加者からデータ取得と利用目的の同意を取得するタイミングは二回ある。モデル事業参加者が地域ウォレットアプリで各機能を利用し始める際に、個人情報の利用目的を明示し、同意を取得する。

①　初回起動時（アカウント登録前）

②　決済事業者とのサービス登録前

②　決済事業者との契約関係

商工会議所がモデル事業協力店舗を募集し、決済事業者へモデル事業の内容と参加店舗リストを事前共有する。加盟店契約は決済事業者と各店舗の間で締結する。決済事業者との接続に関する契約（接続事業者となる契約）は決済事業者とシステム開発会社等の間で締結する。QR コード情報・モデル事業協力店舗情報はモデル事業協力店舗や、社団法人から商工会議所を通じてシステム開発会社等へ連携される。

③　複数ステークホルダ間で個人情報を取扱う方法

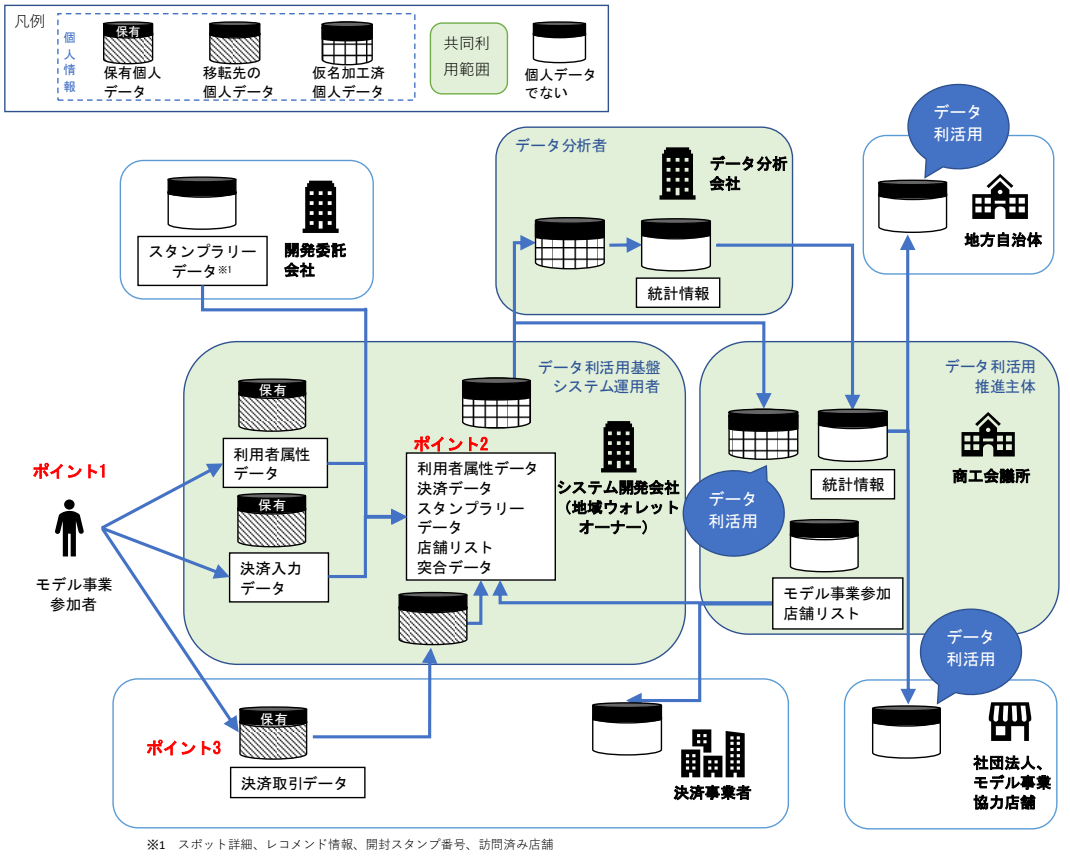
システム開発会社等（データ利活用基盤システム運用者）が集めたデータは、商工会議所（データ利活用推進主体）や、データ分析会社等（データ分析者）に連携される。連携方法としては、データ利活用に関わる契約（共同利用）を締結している。

ビジネス関係図記載時の留意点（観光支援モデル）

ポイント	説明
1	ステークホルダ間でのデータ連携において、モデル事業参加者のプライバシーを最大限考慮し、委託、共同利用、第三者提供のうち、適切なデータ受け渡しの法的根拠を検討する。
2	商工会議所（データ利活用推進主体）は、決済事業者と各ステークホルダ間の契約を検討する上で、加盟店開拓や加盟店管理をどの主体が行うか、加盟店に関するデータをどこから入手するのか等を明確にする。

4.6.4 データリソースマップ（観光支援モデル）

図表 36　データリソースマップ（観光支援モデル）



データリソースマップ記載時の留意点（観光支援モデル）

ポイント	説明
1	モデル事業参加者から個人情報の変更依頼・削除依頼があった際には、共同利用者に連携したデータまでを変更・削除対象とする。但し、決済事業者との間で発生した取引データの削除は、関連法制に則り削除の可否が変わる。統計情報はある時点のスナップショットであるため、遡求する必要はない。
2	共同利用者間では、個人データを加工した仮名加工情報を連携しデータ分析、データ利活用する。その際、個人を特定できるマスタは共同利用者には連携しない。 またデータの取扱いは個人情報同等の取扱いとする。
3	決済事業者は、地域ウォレットを通して決済を実施している中で、モデル事業参加者から決済情報（決済取引データ）を取得している。

① 保持データの整理（観光支援モデル）

図表 37 商工会議所 保持データ（観光支援モデル）

No	保有者	データの内容	データの種類
1	商工会議所	モデル事業参加店舗リスト （加盟店名、加盟店住所等）	個人情報を 含まない
2	システム 開発会社	突合データ（決済データ、利用者属性データ、スタンプラリーデータ、店舗リストを突合したデータ）	仮名加工情報
3	データ分析会社等	突合データを分析し統計データにしたもの	統計情報

図表 38 システム開発会社等 保持データ（観光支援モデル）

No	保有者	データの内容	データの種類
1	システム 開発会社	アプリ利用者の利用者属性データ （氏名、住所、電話番号等）	個人情報
2	システム 開発会社	アプリ利用者の決済入力データ （入力金額、決済店舗 ID、決済日時等）	個人情報
3	システム 開発会社	突合データ（決済データ、利用者属性データ、スタンプラリーデータ、店舗リストを突合したデータ）	仮名加工情報
4	決済事業者	決済取引データ （決済取引連番・精算情報・取引情報）	個人情報

図表 39 データ分析会社等 保持データ（観光支援モデル）

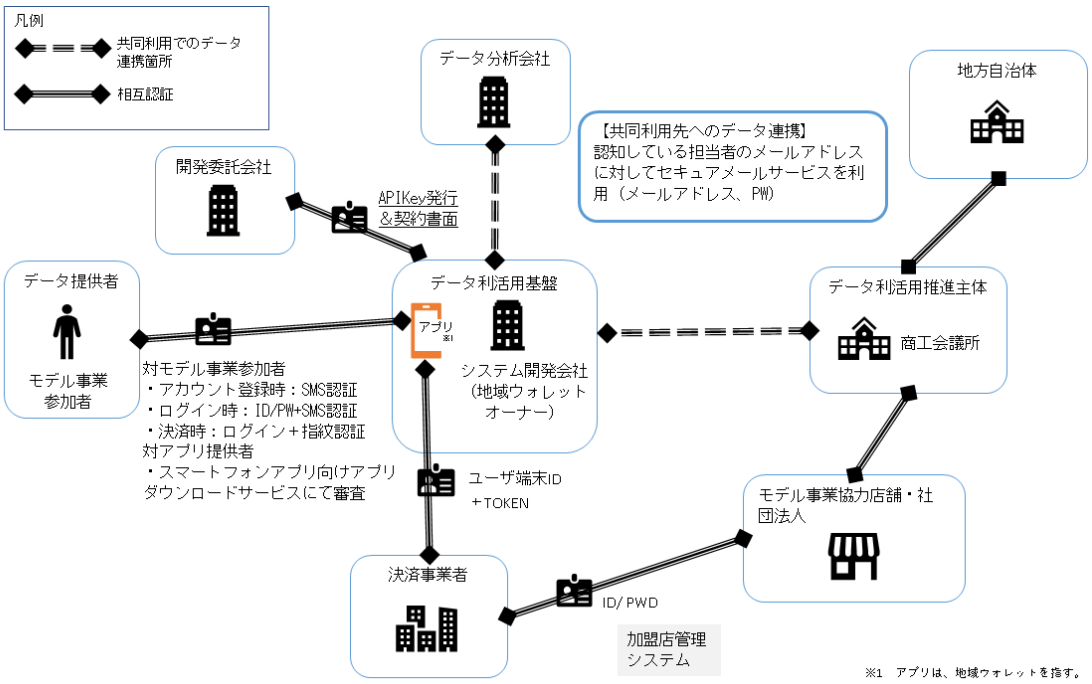
No	保有者	データの内容	データの種類
1	システム 開発会社	突合データ（利用者属性データ、決済データ、スタンプラリーデータ、店舗リストを突合したデータ）	仮名加工情報
2	データ分析会社等	突合データを分析し統計データにしたもの	統計情報

図表 40 決済事業者 保持データ（観光支援モデル）

No	保有者	データの内容	データの種類
1	決済事業者	決済取引データ（決済取引連番、取引情報、精算情報）	個人情報

4.6.5 トラストリソースマップ（観光支援モデル）

図表 41　トラストリソースマップ（観光支援モデル）



図表 42　各ステークホルダ間での認証有無（観光支援モデル）

関係 A	関係 B	A から B の認証	B から A の認証	認証
モデル事業参加者	システム開発会社等（地域ウォレット）	参加者はスマートフォンアプリ向けアプリダウンロードサービスからアプリをインストールすることで B を確認している。	SMS 認証（電話番号認証）でモデル事業参加者の本人確認は実施している。	相互認証
システム開発会社等（地域ウォレット）	決済事業者	決済事業者との接続設定をする際に認証している。	口座登録時のユーザ端末 ID と、トークンを使っての認証している。	相互認証
システム開発会社	決済事業者	お互いの信頼性は契約時に担保している。		相互認証
システム開発会社	商工会議所	お互いの信頼性は契約時に担保している。 データのやり取りについては、セキュアメールにて実施している。		相互認証
システム開発会社	データ分析会社	お互いの信頼性は契約時に担保している。 データのやり取りについては、セキュアメールにて実施している。		相互認証
システム開発会社	システム開発委託会社	お互いの信頼性は契約時に担保している。		相互認証

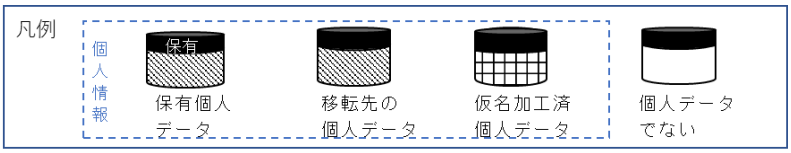
関係 A	関係 B	A から B の認証	B から A の認証	認証
モデル事業 協力店舗・ 社団法人	決済事業者 （加盟店管理 システム）	SSL 通信でアクセスしているため、加盟店管理システムであることは認知できている。	加盟店管理システムから払いだされた ID/PW で認証している。	相互認証
モデル事業 協力店舗・ 社団法人	商工会議所	お互いの信頼性は契約時に担保している。		相互認証
商工会議所	地方自治体	お互いの信頼性は契約時に担保している。		相互認証

データ利活用推進主体から共同利用者へデータ共有する際の実施手順

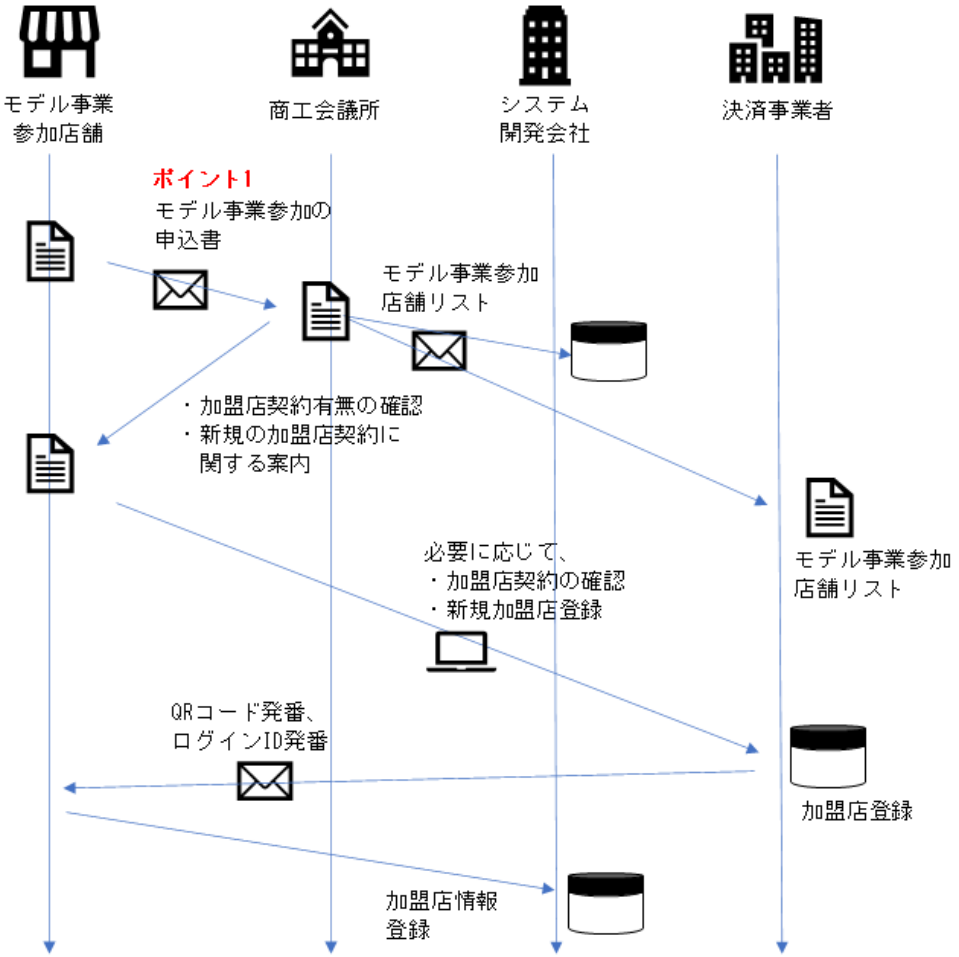
１．決済データ・スタンプラリーデータ・利用者属性データ・店舗リストの突合データを仮名加工処理し、仮名加工情報とする。
２．社内での持出申請フローに従い実施する。
　－１．仮名加工情報の暗号化処理を実施する。
　－２．個人情報保護責任者に対して持出許可をもらう。
　－３．セキュアメールにて、共同利用者に対して送付する。
３．共同利用者の受信確認後、送付したデータは削除する。
４．個人情報貸し出し一覧へ記載し、破棄もしくは返却を確認してから
　クローズする。

4.6.6 データフローシーケンス（観光支援モデル）

データフローシーケンスを基に、実際のモデル事業の流れを時系列にまとめる。以下は各図表で使用するアイコンであるが、それぞれのアイコンを区別することにより、各個人データの保有者、連携先、及び加工の有無を整理する。



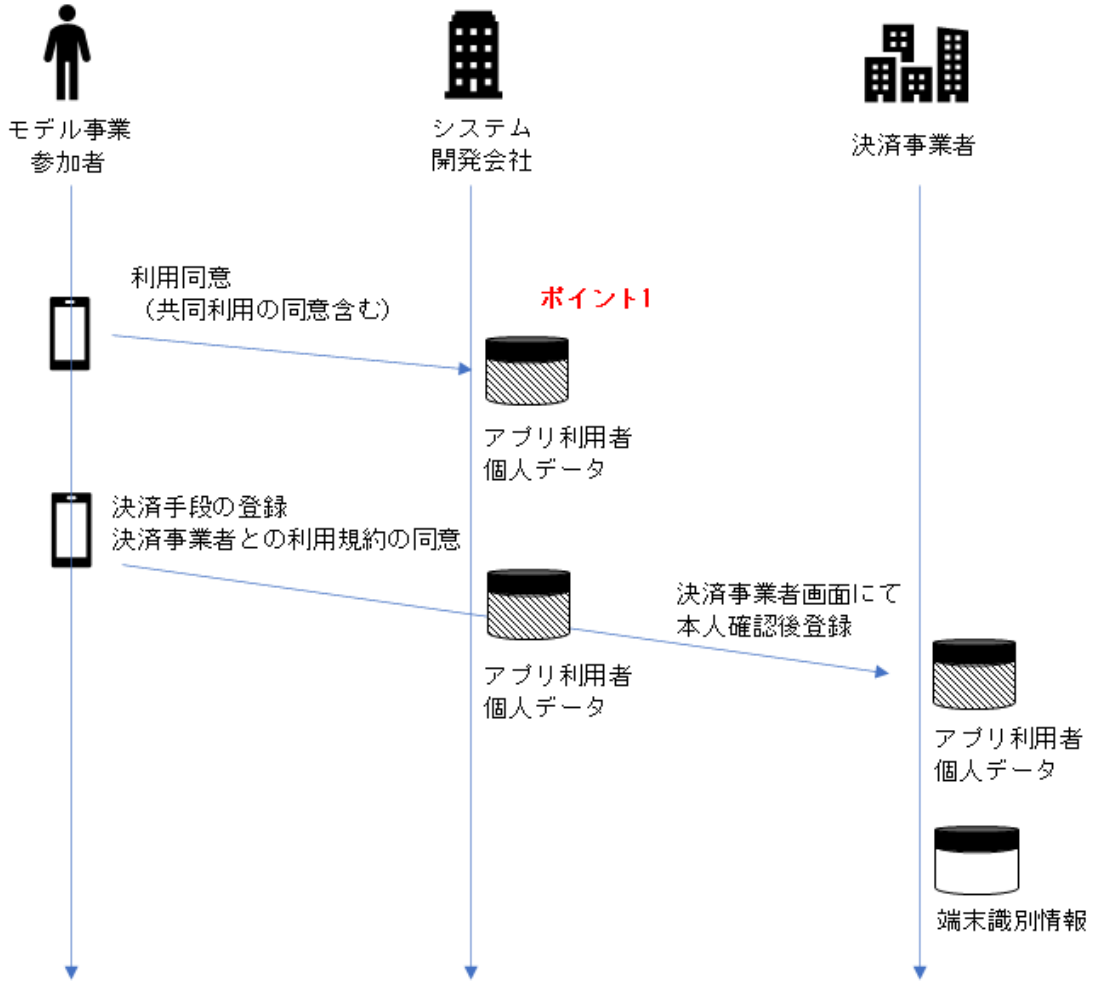
図表 43　データフローシーケンス
＜モデル事業参加店舗募集＞（観光支援モデル）



データフローシーケンス＜モデル事業参加店舗募集＞記載時の留意点（観光支援モデル）

ポイント	説明
1	商工会議所はモデル事業参加店舗の募集を行い、決済事業者へモデル事業の内容と参加店舗リストを事前共有する。モデル事業参加店舗は、必要に応じて決済事業者に対して加盟店登録の申請を行う。

図表 44　データフローシーケンス＜会員登録＞（観光支援モデル）

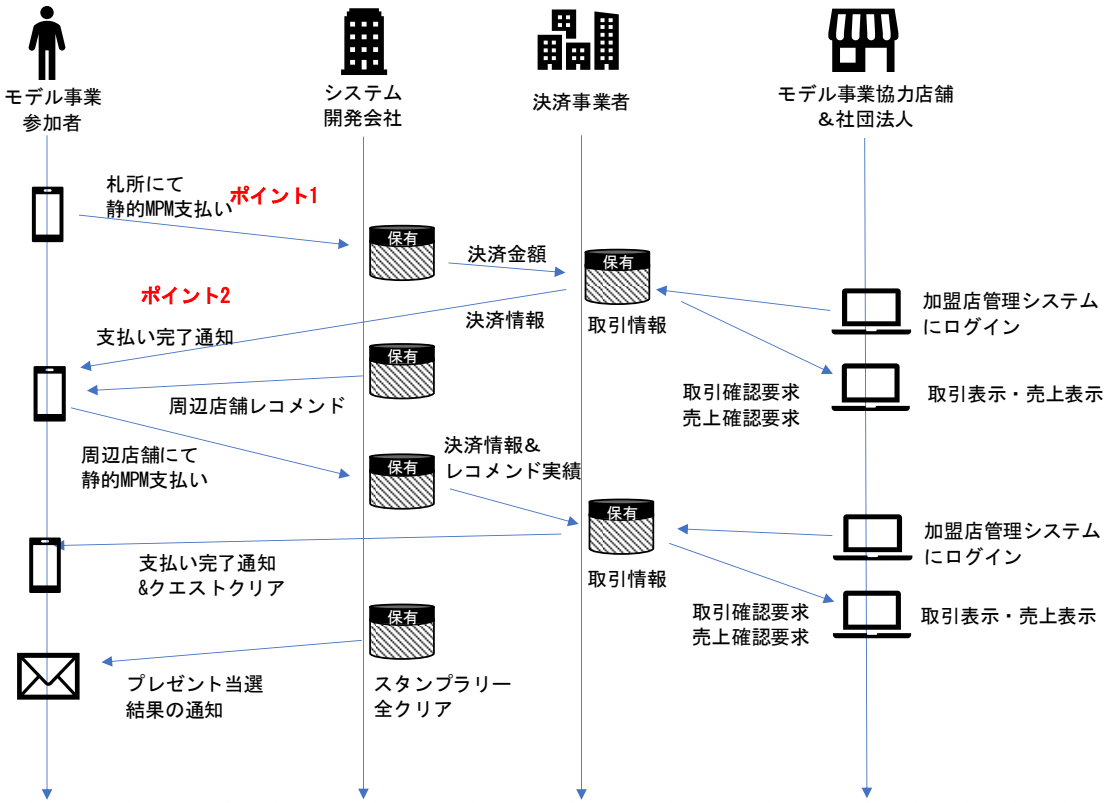


データフローシーケンス＜会員登録＞記載時の留意点（観光支援モデル）

ポイント	説明
1	個人情報の収集を始める前には、あらかじめ本人に対し利用目的の明示が必要となる。※詳細は、4.8 (2) 4「直接書面等による取得」を参照

図表 45　データフローシーケンス

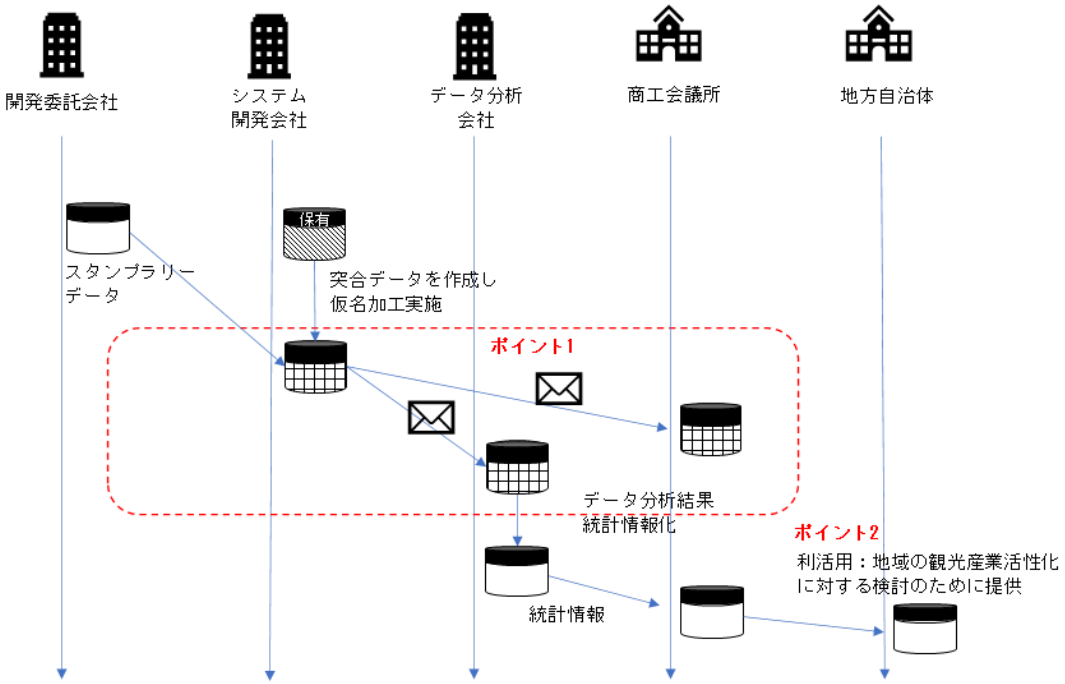
＜札所募金～スタンプラリー終了まで＞（観光支援モデル）



データフローシーケンス＜札所募金～終了まで＞記載時の留意点（観光支援モデル）

ポイント	説明
1	支払い情報が取引実行に使用されるため、利用目的への記載が必要となる。
2	決済事業者からの取得を明示するのが適切な項目がある場合には、地域ウォレットのプライバシーポリシーに、決済事業者から連携されるデータ項目を記載し、同意を取得する。

図表 46　データフローシーケンス＜突合データ連携～分析＞（観光支援モデル）



データフローシーケンス＜突合データ連携～分析＞記載時の留意点（観光支援モデル）

ポイント	説明
1	データ利活用するために仮名加工を施した個人データを共同利用先に連携する。共同利用するものの範囲・共同利用者の利用目的・共同利用する個人データの項目・個人データの管理ついて責任を有するものについて本人に通知または容易に知りうる状態におく必要がある。また、仮名加工情報は本人を識別することを目的としてほかの情報と照合してはならない。 ※詳細は、4.8 (4) 4「第三者提供に該当しない場合」を参照
2	統計情報のみを利活用する場合は、その利用目的をユーザに公表等する必要はない。

4.6.7 法制関連図

各ステークホルダ間で締結する契約及び留意すべき法律等は次のようなものが挙げられる。

ここで挙げたものが各ステークホルダ間で遵守できているか再確認する必要がある。

図表 47　法制関連図（観光支援モデル）

	モデル事業参加者	システム開発会社	開発委託会社	決済事業者	社団法人・ モデル事業協力店舗	データ分析会社	商工会議所	地方自治体
モデル事業 参加者	NA	個人情報保護法 （個人情報取扱事業者） アプリ約款同意	取引規定への同意 （アプリ内で実施）	個人情報保護法 （個人情報取扱事業者） 取引規定への同意 （アプリ内で実施）	売買契約	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー）	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー） 景品表示法	-
システム 開発会社	個人情報保護法 （個人情報取扱事業者） アプリ約款同意	NA	委託契約（スタンプラリー機能開発）	決済事業者との加盟契約（接続事業者） 資金決済法	-	データ利活用の契約 （共同利用）	委託契約 （データ収集） データ利活用の契約 （共同利用）	-
開発委託 会社	取引規定への同意 （アプリ内で実施）	委託契約（スタンプラリー機能開発）	NA	-	-	-	-	-
決済事業者	個人情報保護法 （個人情報取扱事業者） 取引規定への同意 （アプリ内で実施）	決済事業者との加盟契約（接続事業者） 資金決済法	-	NA	決済事業者との 加盟契約	-	-	-

	モデル事業参加者	システム開発会社	開発委託会社	決済事業者	社団法人・ モデル事業協力店舗	データ分析会社	商工会議所	地方自治体
社団法人・ モデル事業協力店舗	売買契約	-	-	決済事業者との 加盟契約	NA	-	スタンプラリー参加の申込み	-
データ分析会社等	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー）	データ利活用の契約 （共同利用）	-	-	-	NA	委託契約 （データ分析） データ利活用の契約 （共同利用）	-
商工会議所	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー） 景品表示法	委託契約 （データ収集） データ利活用の契約 （共同利用）	-	-	スタンプラリー参加の申込み	委託契約 （データ分析） データ利活用の契約 （共同利用）	NA	観光産業の活性化に関する調査
地方自治体	-	-	-	-	-	-	観光産業の活性化に関する調査	NA

4.7 交通支援モデルの例

4.7.1 交通支援モデルの概要

交通支援モデルでは、福島県にて地域交通問題解決のためのデータ利活用事業を実施した。実施したモデル事業を基にユースケースシナリオテンプレートを記載しているが、一部事務局が担当したロール等は抽象化し、実運用を見据えた時に想定される企業・団体に置き換えて記載する。

① 地域課題

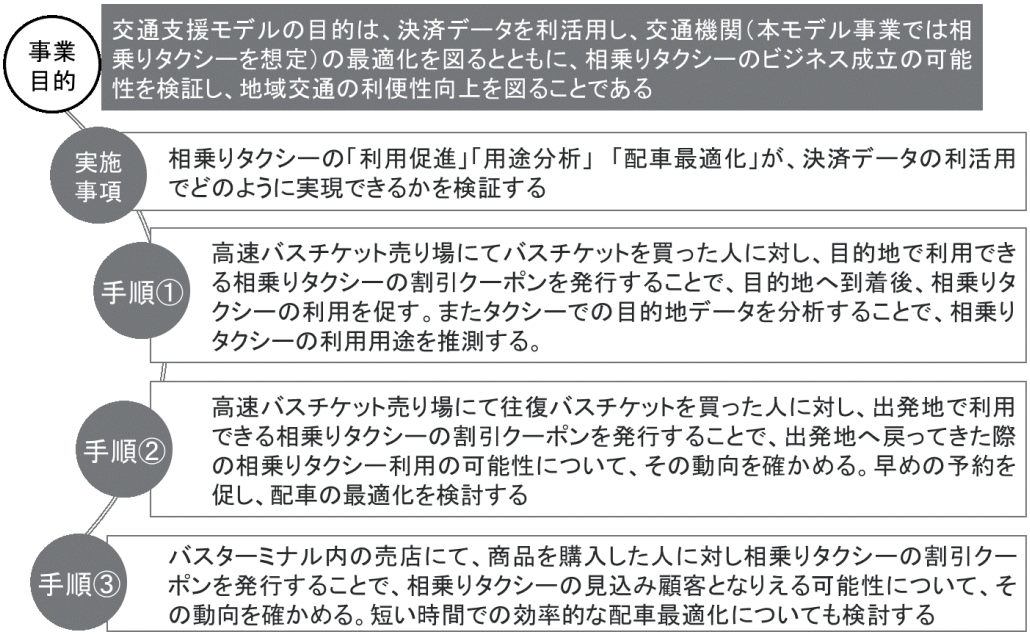
- 地域交通の持続可能性の観点より、自家用車以外の地域の交通手段を強化する必要がある。
- 相乗りタクシー[40]等スモールスタートできる交通手段でビジネス化成立の可能性を検証したい。

② 実施事項

決済データを利活用することで交通機関（今回のモデル事業では相乗りタクシーを想定）の最適化を図るとともに、相乗りタクシーのビジネス成立の可能性を検証し、地域交通の利便性向上を図る。

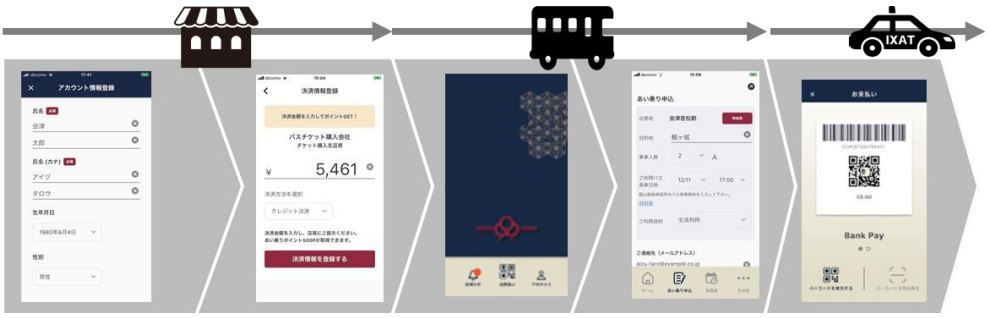
[40] 相乗りタクシーとは、配車アプリを活用して複数の利用者を 1 台のタクシーにマッチングし、タクシーを一人で利用するより割安な運賃で利用可能にするサービス。これにより、「タクシーの運賃は高い」という理由で利用を控えていた方にも利用しやすいタクシーサービスを目指す。事業者・ドライバにとっては、複数の利用者を効率的に運送することが可能になる。
参照 URL：https://www.mlit.go.jp/report/press/jidosha03_hh_000273.html

図表 48　概要説明（交通支援モデル）



モデル事業参加者には、スマートフォンアプリ（地域ウォレット）の利用を通してデータ収集に協力を依頼した。

図表 49　モデル事業の流れ（交通支援モデル）



モデル事業参加者は、スマートフォンアプリ（地域ウォレット）から事前に会員登録を行い、チケット売り場で高速バスチケットを購入する。購入後、決済データを基に相乗りタクシーがレコメンドされ、バス乗車中に相乗りタクシーの予約申し込みを行う。バスが停留所に到着後、予約した相乗りタクシーで目的地まで移動する。相乗りタクシーの旅行代金は、相乗りタクシー乗車時に地域ウォレットを通じて決済する。地域ウォレットは、モデル事業参加者の決済情報、相乗りタクシー予約情報等を紐付けてデータ取得する。

4.7.2 ステークホルダリスト（交通支援モデル）

図表 50　ステークホルダリスト（交通支援モデル）

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
交通事業者[41]等	有	継続可能な地域交通課題について考えている主体者。仮名加工したデータをシステム開発会社等から取得し、相乗りタクシービジネス化検討を行う。	データ利活用推進主体	
システム開発会社[42]等	有	地元のシステム開発会社等。 地域ウォレットのオーナー及び、配車手配支援システムのオーナー。 モデル事業参加者情報、相乗りタクシー申し込み情報、地域ウォレットを通して取得される決済入力データの保有者。 利用者属性データ、決済データ、相乗りタクシー申し込みデータの突合した情報の作成者。	データ利活用基盤システム運用者	地域ウォレット事業者
データ分析会社[43]等	有	地元のデータ分析会社（ベンチャー）等。 仮名加工したデータをシステム開発会社等から取得し、ビジネス化検討のための分析・検討を行う。	データ分析者	
モデル事業参加者	無	地域の地域ウォレットの利用者。 チケット販売店にて、高速バスチケットを購入し、バス乗車中にバス到着後の移動手段を予約する。	データ提供者	
決済事業者[44]	有	決済用の API 提供者・電子決済代行業者 加盟店開拓をしており、加盟店の情報を保有。	データ提供者	決済事業者
旅行代理店等	有	手配型旅行を提供。 相乗りタクシー業務は交通事業者に委託。 相乗りタクシー申込画面は地域ウォレットに実装。	データ提供者	－

ポイント 1

ポイント 2

[41] モデル事業では事務局を請け負った 3 社がデータ推進主体のロールを担当した。

[42] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。

[43] モデル事業では事務局を請け負った 3 社のうちの 1 社が担当した。

[44] モデル事業ではポイントサービスを使用した。

ステークホルダ名称	個人情報取扱有無	概要（主に個人情報保護法での位置づけ）	ロール	地域におけるデータ利活用のためのコード決済情報等の取得に係る標準 API ガイドラインの読者
		相乗りタクシー申込情報の保有者。		
地方自治体	無	交通事業者から統計情報を受領して、地域交通の持続可能性のためにデータ利活用を行う。	データ利活用者	

配車手配支援システムとは、相乗りタクシー申し込み情報（申込者と行き先）を基に配車手配（どの車にだれを乗せるか）を行うために交通事業者が使用するシステムのことを指す。

今モデル事業では、スケジュールの関係から旅行代理店の手配型旅行という建付けにて相乗りタクシーを実現した。交通事業者のサービスとして相乗りタクシーを実施する事は可能である。

① 決済情報の保有個人データ[45]

図表 51　データ利活用する項目の個人データ保有者

	データ保有者		データ利活用の対象項目
	システム開発会社等	決済事業者	
地域ウォレット ID に紐付く決済金額	●	－	対象
地域ウォレット ID に紐付く決済結果	●	－	対象
地域ウォレット ID に紐付く決済日時	●	－	対象
地域ウォレット ID に紐付く決済時の	－	－	－

[45] 保有個人データの法的な定義については、通則編（2-7 保有個人データ）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf

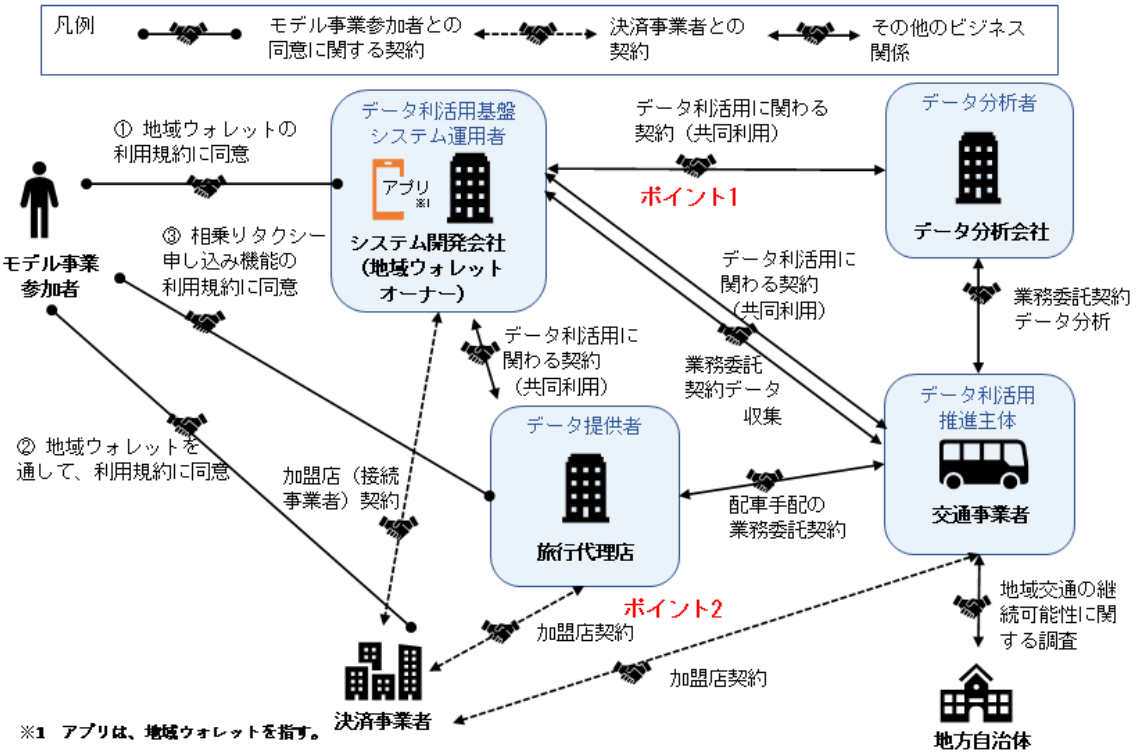
位置情報			
地域ウォレット ID に紐付く決済店舗 ID	●		対象
取引情報（決済取引データ）	－	●	－
精算情報（決済取引データ）	－	●	－

ステークホルダリスト記載時の留意点（交通支援モデル）

ポイント	説明
1	「決済情報」が地域ウォレットの保有個人データとなるのかを判断するため、以下二点を確認する。 • 決済事業者との契約 • 決済時の画面を地域ウォレットが提供していることがモデル事業参加者目線で容易に判別できること（決済事業社が提供する画面での決済の場合等においては、決済情報が地域ウォレットの保有個人データとならない可能性が高いため） 交通支援モデルでは、決済入力データは、地域ウォレット＝システム開発会社等の保有個人データとなる。
2	「データ提供者」を洗い出す。 連携が必要なデータが何かを洗い出し、データを収集するための契約を締結する必要がある。

4.7.3 ビジネス関係図（交通支援モデル）

図表 52　ビジネス関係図（交通支援モデル）



①　モデル事業参加者との契約関係

モデル事業参加者からデータ取得と利用目的の同意を取得するタイミングは三回ある。モデル事業参加者が地域ウォレットアプリで各機能を利用し始める際に、利用目的を明示し、同意を取得する。

①　初回起動時（アカウント登録前）

②　決済事業者とのサービス登録前

③　相乗りタクシー申し込みサービス利用前

② 決済事業者との契約関係

システム開発会社等が決済事業者との接続に関する契約（接続事業者となる契約）を締結し、決済事業者が各店舗と加盟店契約を締結する。

③ 複数ステークホルダ間で個人情報を取扱う方法

システム開発会社等（データ利活用基盤システム運用者）が集めたデータは、交通事業者（データ利活用推進主体）や、データ分析会社等（データ分析者）に連携される。連携方法としては、データ利活用に関わる契約（共同利用）を締結している。

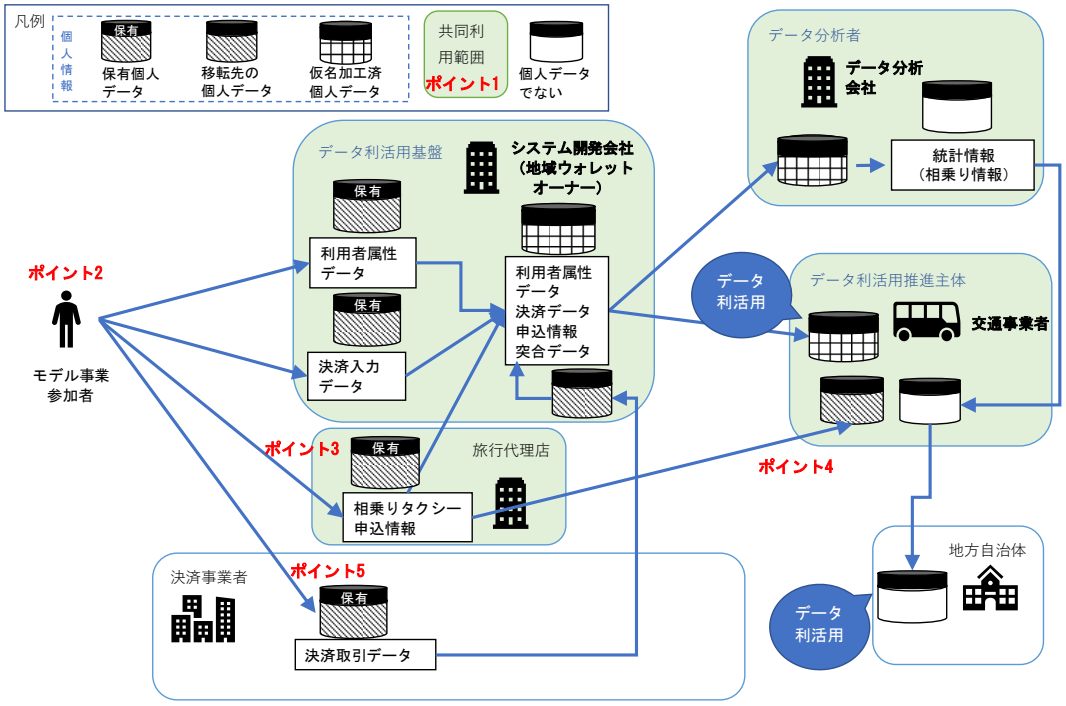
ビジネス関係図記載時の留意点（交通支援モデル）

ポイント	説明
1	ステークホルダ間でのデータ連携において、モデル事業参加者のプライバシーを最大限考慮し、委託、共同利用、第三者提供のうち、適切なデータ受け渡しの法的根拠を検討する。
2	決済事業者との契約を締結する上で、加盟店開拓や加盟店管理をどの主体が行うか、加盟店に関するデータをどこから入手するのか等を明確にする。

4.7.4 データリソースマップ（交通支援モデル）

データリソースマップを用いて、ビジネス関係図と同じ配置の状態で各ステークホルダのデータ保持と受け渡しを記載した。

図表 53　データリソースマップ（交通支援モデル）



データリソースマップ記載時の留意点（交通支援モデル）

ポイント	説明
1	共同利用者間では、個人データを加工した仮名加工情報を連携しデータ分析、データ利活用する。その際、個人を特定できるマスタは共同利用者には連携しない。またデータの取扱いは個人情報同等とする。
2	モデル事業参加者から個人情報の変更依頼・削除依頼があった際には、共同利用者に連携したデータまでを変更・削除対象とする。但し、決済事業者との間で発生した取引データの削除は、関連法制に則り削除の可否が変わる。統計情報はある時点のスナップショットであるため、遡求する必要はない。
3	相乗りタクシー申し込みは地域ウォレットを通して行うが、旅行代理店の手配型旅行企画の申込のため、この場合、データ保有者は旅行代理店となる。
4	相乗りタクシー申し込み情報を基に配車業務を行うため、交通事業者には個人データが連携される。

5	決済事業者は、地域ウォレットを通して決済を実施している中で、モデル事業参加者から決済情報（決済取引データ）を取得している。

① 保持データの整理（交通支援モデル）

図表 54 交通事業者 保持データ（交通支援モデル）

No	保有者	データの内容	データの種類
1	システム開発会社等	アプリ利用者の利用者属性データ（電話番号を一意となるランダムな値に変更したもの、郵便番号、年齢等）	仮名加工情報
2	システム開発会社等	アプリ利用者の決済入力データ（入力金額、決済店舗 ID、決済日時等）	仮名加工情報
3	旅行代理店等	アプリ利用者の相乗りタクシー申込データ（氏名、目的地、参加人数、連絡先メールアドレス等）	個人情報・仮名加工情報
4	データ分析会社等	利用者属性データ、決済データ、相乗りタクシー申込情報を突合しデータ分析、統計化した情報	統計情報

図表 55 システム開発会社等保持データ（交通支援モデル）

No	保有者	データの内容	データの種類
1	システム開発会社等	アプリ利用者の利用者属性データ（氏名、住所、電話番号等）	個人情報 仮名加工情報
2	システム開発会社等	アプリ利用者の決済入力データ（入力金額、決済店舗 ID、決済日時等）	個人情報 仮名加工情報
3	旅行代理店等	アプリ利用者の相乗りタクシー申込データ（目的地、参加人数）	仮名加工情報
4	決済事業者	決済取引データ（決済取引連番、取引情報、精算情報）	個人情報

図表 56 旅行代理店 保持データ（交通支援モデル）

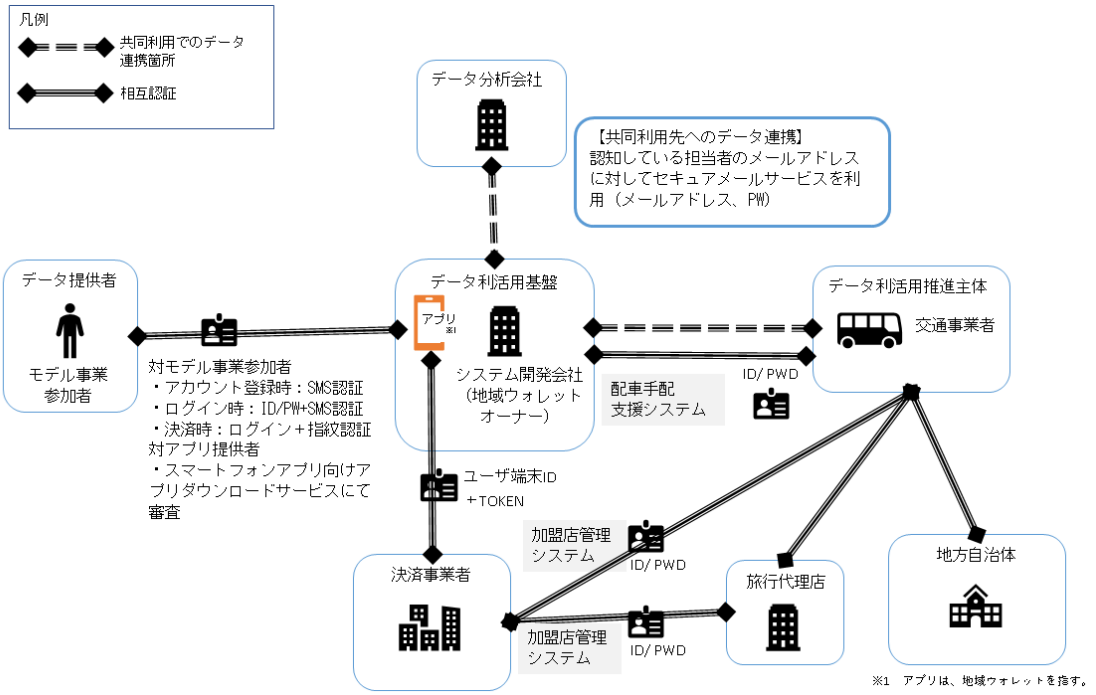
No	保有者	データの内容	データの種類
1	旅行代理店等	アプリ利用者の相乗りタクシー申込データ（氏名、目的地、参加人数、連絡先メールアドレス等）	個人情報

図表 57 決済事業者 保持データ（交通支援モデル）

No	保有者	データの内容	データの種類
1	決済事業者等	決済取引データ（決済取引連番、取引情報、精算情報）	個人情報

4.7.5 トラストリソースマップ（交通支援モデル）

図表 58　トラストリソースマップ（交通支援モデル）



図表 59　各ステークホルダ間での認証有無（交通支援モデル）

関係 A	関係 B	A から B の認証	B から A の認証	認証
モデル事業参加者	システム開発会社等（地域ウォレット）	参加者はスマートフォンアプリ向けアプリダウンロードサービスからアプリをインストールすることで B を確認している。	SMS 認証（電話番号認証）でモデル事業参加者の本人確認は実施している。	相互認証
システム開発会社等（地域ウォレット）	決済事業者	決済事業者との接続設定をする際に認証している。	口座登録時のユーザ端末 ID と、トークンを使っての認証している。	相互認証
システム開発会社等	決済事業者	お互いの信頼性は契約時に担保している。		相互認証
システム開発会社等	交通事業者等	お互いの信頼性は契約時に担保している。データのやり取りについては、セキュアメールにて実施している。		相互認証

関係 A	関係 B	A から B の認証	B から A の認証	認証
システム 開発会社等	データ分析 会社等	お互いの信頼性は契約時に担保している。 データのやり取りについては、セキュアメールにて実施している。		相互 認証
システム開発会社等（配車手配支援システム）	交通事業者等	アクセス制御を実施している。（交通事業者の拠点からのみ接続可能）	配車手配支援システムの ID は、交通事業者から指定を受けてアカウントの払い出しを行っている。	相互 認証
交通事業者・旅行代理店等	決済事業者（加盟店管理システム）	SSL 通信でアクセスしているため、加盟店管理システムであることは認知できている。	加盟店管理システムから払いだされた ID/PW で認証している。	相互 認証
交通事業者等	旅行代理店等	お互いの信頼性は契約時に担保している。		相互 認証
交通事業者等	地方自治体	お互いの信頼性は契約時に担保している。		相互 認証

データ利活用推進主体から共同利用者・委託先へデータ共有する際の実施手順

1．決済データ・相乗り申込データ・利用者属性データの突合データを

　仮名加工処理し、仮名加工情報とする。

2．社内での持出申請フローに従い実施する。

　－1．仮名加工情報の暗号化処理を実施する。

　－2．個人情報保護責任者に対して持出許可をもらう。

　－3．セキュアメールにて、共同利用者に対して送付する。

3．共同利用者の受信確認後、送付したデータは削除する。

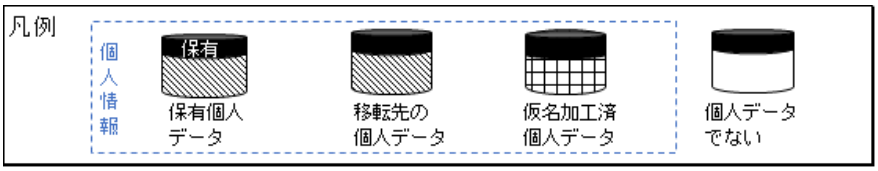
4．個人情報貸し出し一覧へ記載し、破棄もしくは返却を確認してから

　クローズする。

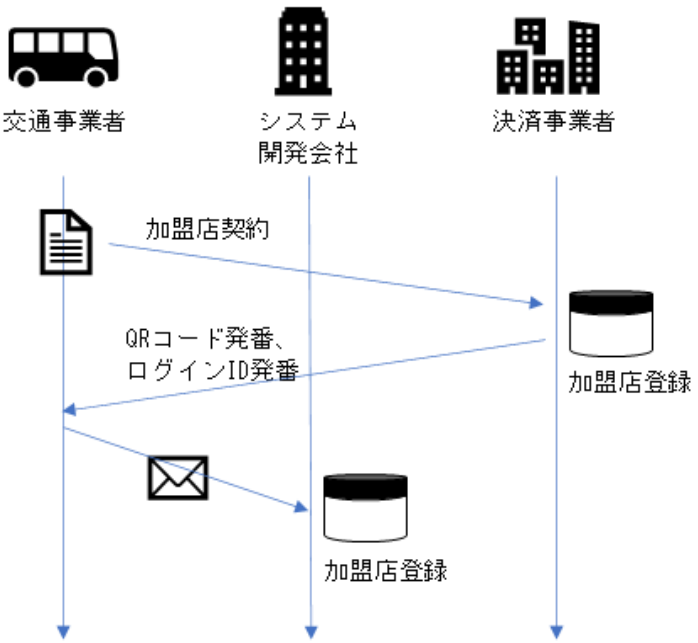
4.7.6 データフローシーケンス（交通支援モデル）

データフローシーケンスを基に、実際のモデル事業の流れを時系列にまとめる。

以下は各図表で使用するアイコンであるが、それぞれのアイコンを区別することにより、各個人データの保有者、連携先、及び加工の有無を整理する。

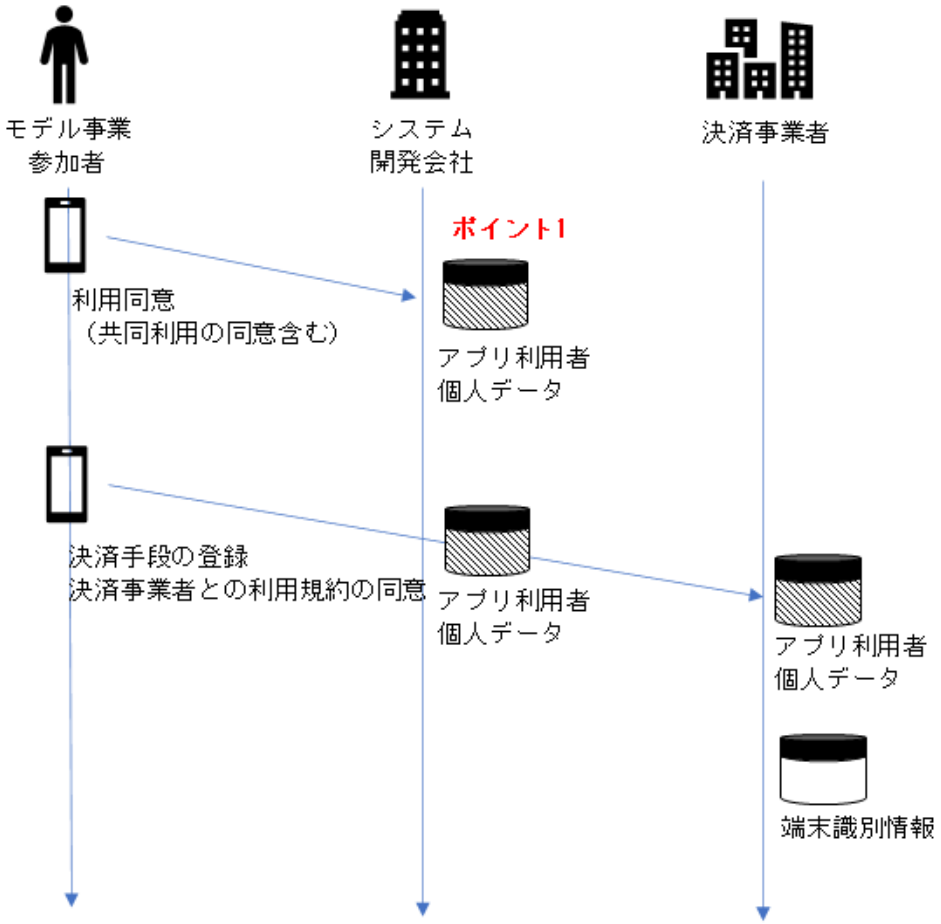


図表 60　データフローシーケンス＜加盟店契約＞（交通支援モデル）



交通事業者等は、決済事業者と加盟店契約を締結し、QR コードが連携される。交通事業者は QR コード情報をシステム開発会社等へ共有し、システム開発会社等は加盟店情報を登録する。

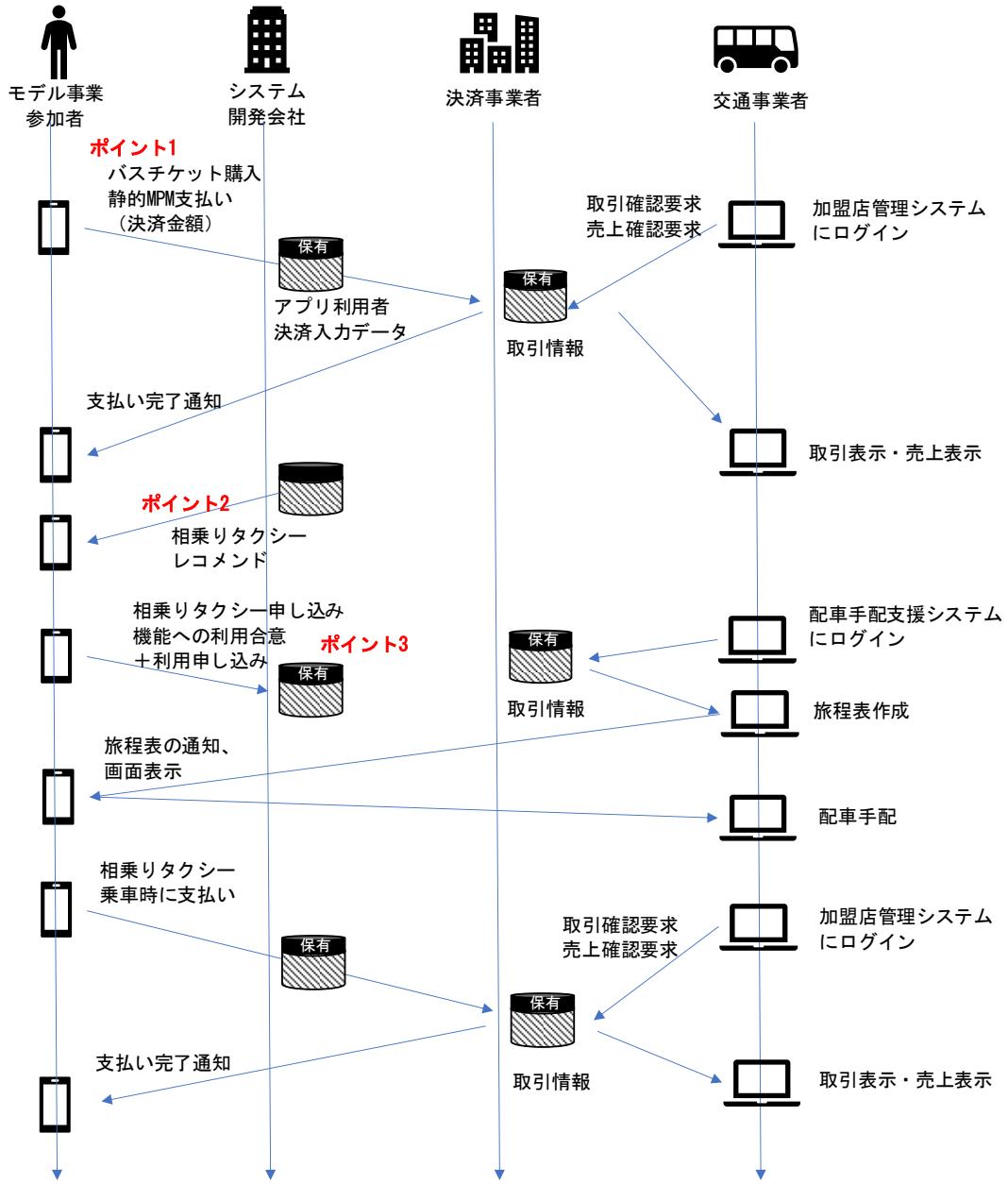
図表 61　データフローシーケンス＜会員登録＞（交通支援モデル）



データフローシーケンス＜会員登録＞記載時の留意点（交通支援モデル）

ポイント	説明
1	個人情報の収集を始める前には、あらかじめ本人に対し利用目的の明示が必要となる。※詳細は、4.8 (2) 4「直接書面等による取得」を参照

図表 62　データフローシーケンス＜購入～相乗り支払い＞（交通支援モデル）



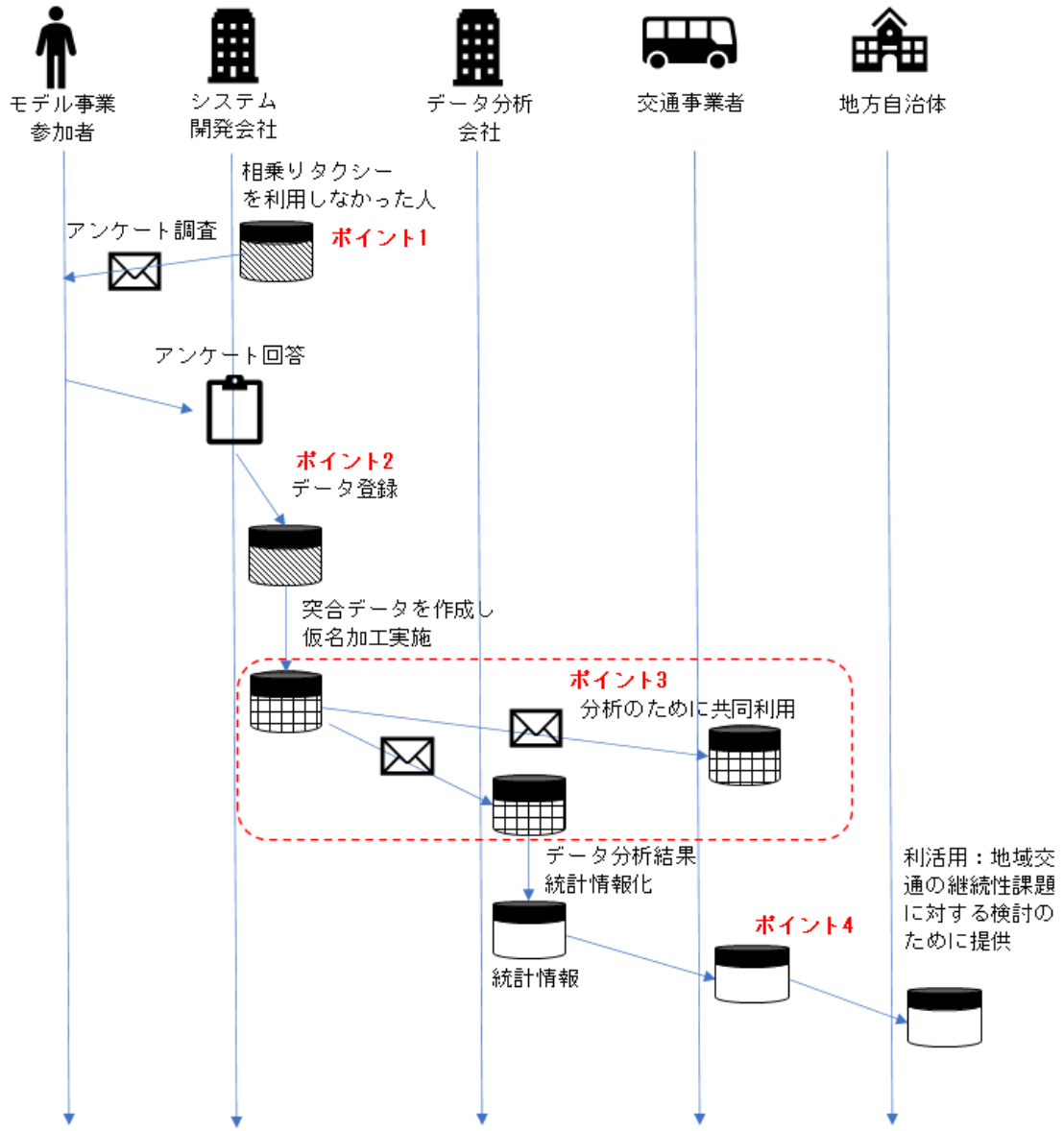
データフローシーケンス＜購入～相乗り支払い＞

記載時の留意点（交通支援モデル）

ポイント	説明
1	支払い情報が取引実行に使用されるため、利用目的への記載は必要となる。

ポイント	説明
2	相乗りタクシーサービス紹介のために個人情報を使用しているため、利用目的への記載が必要となる。
3	相乗りタクシー申込で取得した個人情報について、利用目的を記載する必要がある。

図表 63　データフローシーケンス＜突合データ連携～分析＞（交通支援モデル）



データフローシーケンス＜突合データ連携～分析＞

記載時の留意点（交通支援モデル）

ポイント	説明
1	相乗りタクシー申し込み機能を利用しなかった人を対象にアンケートを送付する場合は、利用目的に記載する必要がある。

ポイント	説明
2	相乗りタクシー申し込み機能を利用しなかった人向けのアンケート結果を個人情報として取得することを公表する必要がある。
3	データ利活用するために仮名加工を実施した個人データを共同利用先に連携する。共同利用するものの範囲・共同利用者の利用目的・共同利用する個人データの項目・個人データの管理ついて責任を有するものについて本人に通知または容易に知りうる状態におく必要がある。また、仮名加工情報は本人を識別することを目的としてほかの情報と照合してはならない。 ※詳細は、4.8 (4) 4「第三者提供に該当しない場合」を参照
4	統計情報のみを利活用する場合は、その利用目的をユーザに公表等する必要はない。

4.7.7 法制関連図

各ステークホルダ間で締結する契約及び留意すべき法律や法律で定められた制度は、次のようなものが挙げられる。

ここで挙げたものが各ステークホルダ間で遵守できているか再確認する必要がある。

図表 64　法制関連図（交通支援モデル）

	モデル事業参加者	システム開発会社	決済事業者	交通事業者	旅行代理店	データ分析会社	地方自治体
モデル事業参加者	NA	個人情報保護法 （個人情報取扱事業者） アプリ約款同意・相乗り申し込みサービス 約款同意 景品表示法	個人情報保護法 （個人情報取扱事業者） 取引規定への同意 （アプリ内で実施）	バスチケット （売買契約） 共同利用の同意 （アプリプライバシーポリシー）	手配型旅行契約 旅行業法 共同利用の同意 （アプリプライバシーポリシー）	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー）	－
システム開発会社等	個人情報保護法 （個人情報取扱事業者） アプリ約款同意・相乗り申し込みサービス 約款同意 景品表示法	NA	決済事業者との加盟契約（接続事業者） 資金決済法	委託契約 （データ収集） データ利活用の契約 （共同利用）	地域ウォレットにて申込機能を委託 データ利用の契約 （共同利用）	データ利活用の契約 （共同利用）	－
決済事業者	個人情報保護法 （個人情報取扱事業者） 取引規定への同意 （アプリ内で実施）	決済事業者との加盟契約（接続事業者） 資金決済法	NA	決済事業者との加盟契約	決済事業者との加盟契約	－	－

	モデル事業参加者	システム開発会社	決済事業者	交通事業者	旅行代理店	データ分析会社	地方自治体
交通事業者等	バスチケット （売買契約） 共同利用の同意 （アプリプライバシーポリシー）	委託契約 （データ収集） データ利活用の契約 （共同利用）	決済事業者との加盟契約	NA	手配型旅行 相乗りタクシー業務を委託	委託契約 （データ分析） データ利活用の契約 （共同利用）	地域交通の継続可能性に関する調査
旅行代理店等	手配型旅行契約 旅行業法 共同利用の同意 （アプリプライバシーポリシー）	地域ウォレットにて申込機能を委託 データ利用の契約 （共同利用）	決済事業者との加盟契約	手配型旅行 相乗りタクシー業務を委託	NA	－	－
データ分析会社等	個人情報保護法 （共同利用者） 共同利用の同意 （アプリプライバシーポリシー）	データ利活用の契約 （共同利用）	－	委託契約 （データ分析） データ利活用の契約 （共同利用）	－	NA	－
地方自治体	－	－	－	地域交通の継続可能性に関する調査	－	－	NA

4.8 個人情報保護法観点で遵守すべきこと

個人情報取扱事業者となる可能性が高いステークホルダとしては、主にデータ利活用推進主体、データ利活用基盤システム運用者、決済事業者等が挙げられ、業態や対象とするデータの内容等によっては、データ分析者や決済機能を利用する加盟店等も個人情報取扱事業者として規制対象になると考えられる。

個人情報保護法における個人情報取扱事業者が遵守すべき事項の中から、決済情報のデータ利活用において特に注意が必要な以下の 5 点について解説する。

- 個人情報の利用目的（4.8.1）
- 個人情報の取得（4.8.2）
- 個人データの管理（4.8.3）
- 個人データの第三者への提供（4.8.4）
- 保有個人データに関する事項の公表等（4.8.5）

本節では、個人情報保護法に照らして、データ利活用において考慮すべき事項と、今回のモデル事業における対応状況を記載する。

4.8.1 個人情報の利用目的

個人情報の利用目的に関して、今回のモデル事業における対応状況及び本書での取扱いは以下の通りである。

図表 65　個人情報保護法（個人情報の利用目的）

No	利用目的に関連する事項	モデル事業での対応	本書での取扱い
①	利用目的の特定・変更、利用目的による制限	●	●
－	事業の承継	－	－
－	利用目的による制限の例外	－	－

凡例）●：モデル事業での対応有、又は本書での取扱有
－：モデル事業での対応無、又は本書での取扱無

① 利用目的の特定・変更、利用目的による制限

法第 15 条（第 1 項・第 2 項）
1　個人情報取扱事業者は、個人情報を取り扱うに当たっては、その利用の目的（以下「利用目的」という。）をできる限り特定しなければならない。
2　個人情報取扱事業者は、利用目的を変更する場合には、変更前の利用目的と関連性を有すると合理的に認められる範囲を超えて行ってはならない。

法第 16 条（第 1 項）
1　個人情報取扱事業者は、あらかじめ本人の同意を得ないで、前条の規定により特定された利用目的の達成に必要な範囲を超えて、個人情報を取り扱ってはならない。

a. 考慮すべき事項

- 利用目的は、ある程度具体的に特定する必要があり、例えば、「○○事業」、「○○サービス」等においてどのような場面で利用されるかといった点を念頭に、本人が理解できるように記載する。
- 一方で、一般人が変更前後の利用目的を比較して予期できる範囲を超えて、利用目的を広げるには、本人の同意が必要であるが、事後的に同意を取得するのは煩雑である。（ユーザが利用時に必ずアクセスするシステム上で、ユーザの操作によらず同意画面を表示する機能等を実装しない限り、網羅的に同意を取得するのは、極めて困難な状態となる。）
- そのため、過度に利用目的を限定的に記載して、漏れが生じることのないように、初期段階で慎重に検討の上、網羅的に定める必要がある。
- また、複数の事業者において個人情報を利活用する場合等、個人情報を第三者に提供等することを想定している場合には、その趣旨が明らかになるように利用目的を記載する。

b. 今回のモデル事業における対応

- 今回のモデル事業では、当初利用目的を特定するにあたり、個人情報の利用態様について予め検討し、想定しうる利用目的が網羅されるように利用目的を検討し、特定した。その結果、当初特定した利用目的の達成に必要な範囲を超えて個人情報を取扱う事案は発生しなかった。
- 観光支援モデル（埼玉）では、利用目的の特定として地域ウォレットアプリのプライバシーポリシーに以下を記載した。（想定外の連絡が必要になる自体も想定して、当初から利用目的に「本サービスに関する重要なお知らせ等、必要に応じた連絡を行うため」を記載した。）

I. 本サービスの提供・改善・開発のため
- 本サービスを利用したユーザの商品･役務の購入に関する取引の実行のため
- 商品購入時や有料サービス利用時等におけるご請求処理のため
- 本サービスのサービスレベル改善のため
- ユーザの本サービス利用時およびお問い合わせ時等の本人確認のため

＜中略＞
- 本サービスに関する重要なお知らせ等、必要に応じた連絡を行うため

II. 本サービスの不正利用防止のため
- 不正利用防止のため
- 不正利用が発生した場合などに本人確認や連絡を行うため

III. 上記の他、総務省「地域における決済情報等の利活用に係る調査」プロジェクトに採択された観光支援モデルの事業であって、決済情報等の利活用にかかる以下目的のため
- 上記プロジェクトに関する報告資料作成のため
- 上記プロジェクトに関する利用状況の分析、統計データの作成のため

- 今回のモデル事業では、利用目的を変更する事案は生じていない。生活支援モデル（和歌山）では、地域ウォレットアプリのプライバシーポリシーの内、利用目的以外の箇所について変更を行った。その際、変更前と変更後のプライバシーポリシーを A4 用紙に横並びで表示し、変更箇所を強調した資料を作成することで対面での説明時に活用した。利用目的を変更する場合においても、このような対応が考えられる。

4.8.2 個人情報の取得

個人情報の取得に関して、今回のモデル事業における対応状況及び本書での取扱いは以下の通りである。

図表 66　個人情報保護法（個人情報の取得）

No	個人情報の取得に関連する事項	モデル事業での対応	本書での取扱い
①	適正取得	●	●
②	要配慮個人情報の取得	－	●
③	利用目的の通知又は公表	●	●
④	直接書面等による取得	●	●
－	利用目的の通知等をしなくてよい場合	－	－

凡例）●：モデル事業での対応有、又は本書での取扱有
－：モデル事業での対応無、又は本書での取扱無

① 適正取得

法第 17 条（第 1 項）
1　個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

a. 考慮すべき事項

- 本人から直接個人情報を取得する際に、騙すような方法を用いないことはもちろん、第三者を通じて間接的に個人情報を取得する際にも、適正な手段で取得された個人情報であるか留意する必要がある（第三者提供を受ける際の確認義務については「4.8.4④ 第三者提供を受ける際の確認等」参照）。
- 例えば、第三者から個人情報の提供を受ける際に、本人の同意がなく法令上の例外規定等にも該当しないことや不正に取得された個人情報であることを知りつつ（又は容易に知ることができるのに）取得すれば、不正な手段による取得ということになる。

b. 今回のモデル事業における対応

- 今回のモデル事業では、地域ウォレットのプライバシーポリシーにて、個人情報の取得方法（「本サービスの利用にあたってユーザから直接提供いただく方法」と「本サービスの利用に伴い取得する方法（ユーザから直接提供いただくもの以外）」）、取得する項目を全て公表した。また、取得する項目を修正したときは、修正点をわかりやすく説明した。
- 上記の公表は法令上必須とまでは言えないが、特に、「本サービスの利用に伴い取得する方法（ユーザから直接提供いただくもの以外）」については、ユーザが意図しないうちに個人情報を取得することもあるため、ユーザが騙し討ち的に個人情報を取得されたとの不快感を持たないように、慎重に対応したものである。
- 以下は観光支援モデル（埼玉）のプライバシーポリシーの一部である。

2．取得する個人情報の項目について

当社は、本サービスにおいて、本文書1．に記載の利用目的を達成するために、以下に定めるユーザの個人情報を取得します。ユーザによる個人情報の提供は、原則としてユーザの意思によって行われるものですが、提供いただけない場合、本サービスの全部または一部をご利用いただけない場合があります。

(1)　本サービスの利用にあたってユーザから直接提供いただく方法

- ユーザの登録情報
  氏名、性別、生年月日、郵便番号、XX 観光でやりたいこと、XX 観光への同行者との関係、予定移動手段、メールアドレス、その他連絡先に関する情報等
- 決済情報（金額、入力日時、入力店舗情報等）
- ご意見、ご要望、お問い合わせ対応等、本サービスの提供等に付随してユーザから当社に提供される一切の情報

(2)　本サービスの利用に伴い取得する方法（ユーザから直接提供いただくもの以外）

- スタンプラリーサービス内に記載されている電話番号への着信履歴、
- ユーザによる本サービス利用状況（アクセスログ、ご利用の端末情報、ユーザの通信に関わる情報、各種日時情報等）

② 要配慮個人情報[46]の取得

法第 17 条（第 2 項）
2　個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。
(1)　法令に基づく場合
(2)　人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
(3)　公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
(4)　国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。
(5)　当該要配慮個人情報が、本人、国の機関、地方公共団体、第 76 条第 1 項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合
(6)　その他前各号に掲げる場合に準ずるものとして政令で定める場合

規則第 6 条
法第 17 条第 2 項第 5 号の個人情報保護委員会規則で定める者は、次の各号のいずれかに該当する者とする。
(1)　外国政府、外国の政府機関、外国の地方公共団体又は国際機関
(2)　外国において法第 76 条第 1 項各号に掲げる者に相当する者

政令第 7 条
法第 17 条第 2 項第 6 号の政令で定める場合は、次に掲げる場合とする。
(1)　本人を目視し、又は撮影することにより、その外形上明らかな要配慮個人情報を取得する場合
(2)　法第 23 条第 5 項各号に掲げる場合において、個人データである要配慮個人情報の提供を受けるとき。

a. 考慮すべき事項

- 要配慮個人情報については、他の個人情報よりも厳格な取扱いが求められるが、決済情報や購買情報を利活用する場合には要配慮個人情報は必要ないケースも多いと考えられるため、そもそも要配慮個人情報を取得する必要があるか十分検討する。
- 要配慮個人情報を取得する場合には、あらかじめ本人の同意を得なければならないため、意図せず不要な要配慮個人情報が混入しないように留意する。
- 本人から直接取得する場合は、通常、要配慮個人情報を取得する旨の同意も得られていると考えられる。
- 第三者提供の同意には、提供先の特定までは必須ではないが、提供先が要配慮個人情報を取得する旨の同意もあわせて取得しようとする場合には、特定された第三者に提供する旨の同意まで必要と考えられる。
- なお、金融分野の事業者に適用される「金融分野における個人情報保護に関するガイドライン」においては、個人情報保護法上の要配慮個人情報よりも範囲が広い機

[46] 要配慮個人情報の法的な定義等については、通則編（2-3 要配慮個人情報）を参照
参照 URL：https://www.ppc.go.jp/files/pdf/201001_guidelines01.pdf

微（センシティブ）情報について、取得、利用、第三者提供が厳格に制限されている[47]。

b. 今回のモデル事業における対応

- 本事業における分析においては、要配慮個人情報又は機微情報を必要としないと判断されたが、そもそも要配慮個人情報・機微情報を取得し得る状況も発生しておらず、実際に取得することもなかった。

③ 利用目的の通知又は公表

法第 18 条（第 1 項） 1　個人情報取扱事業者は、個人情報を取得した場合は、あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を、本人に通知し、又は公表しなければならない。

a. 考慮すべき事項

- 次項「④ 直接書面等による取得」に該当しない方法で個人情報を取得する場合は、あらかじめその利用目的を公表していることが望ましく、プライバシーポリシー等に利用目的を記載して、ウェブサイト等で公表している事例等が多く見られる。
- 他のステークホルダから個人情報の提供を受ける場合等には、本人へのリーズナブルな通知手段を確保できないケースも少なからず想定され、こうした場合等には、通知よりも公表の方が簡便な手段であると考えられる。
- 公表にあたっては、事業の性質及び個人情報の取扱状況に応じ、合理的かつ適切な方法によらなければならず、ウェブサイトのトップページから 1 回程度の操作で到達できる場所への掲載といった方法等が考えられる。

b. 今回のモデル事業における対応

- 各地域のモデル事業において、事業の実施期間及び地域を限定していること、及び地域ウォレットを利用するためには、アプリをダウンロードする必要がある。ユーザは必ずしもホームページを閲覧するわけではないことを考慮し、利用目的の公表は、アプリ内にプライバシーポリシーを掲載した。その際には、1 クリックの操作で全文が確認できるように配置した。

[47] 機微（センシティブ）情報の法的な定義については、金融分野における個人情報保護に関するガイドライン第 5 条を参照
参照 URL：https://www.fsa.go.jp/common/law/kj-hogo-2/01.pdf

④ 直接書面等による取得

法第 18 条（第 2 項） 2　個人情報取扱事業者は、前項の規定にかかわらず、本人との間で契約を締結することに伴って契約書その他の書面（電磁的記録を含む。以下この項において同じ。）に記載された当該本人の個人情報を取得する場合その他本人から直接書面に記載された当該本人の個人情報を取得する場合は、あらかじめ、本人に対し、その利用目的を明示しなければならない。ただし、人の生命、身体又は財産の保護のために緊急に必要がある場合は、この限りでない。

a. 考慮すべき事項

- 契約書やユーザ入力画面への打ち込み等により、直接本人から個人情報を取得する場合には、あらかじめ、本人に対し、その利用目的を明示しなければならない。
- 「明示」とは、単にウェブサイト等のどこかに掲載しているというだけでは足りず、本人が内容を認識できるように明確に示す方法による必要がある。ウェブサイトやアプリ上において個人情報を取得する場合は、本人が送信ボタン等をクリックする前等にその利用目的（利用目的の内容が示された画面に 1 回程度の操作でページ遷移するよう設定したリンクやボタンを含む。）が本人の目に留まるように配置することが望ましい。
- 直接書面等で取得するケースに限らず、法第 18 条第 1 項の対応（上記③）も含めて、上記の「明示」する方法で対応する方が、共通的な対応となり、結果的に簡便な運用となるケースも考えられる。

b. 今回のモデル事業における対応

- 地域ウォレットでは、アプリダウンロード後、初回起動時にユーザ入力画面を表示する前に利用目的が記載されたプライバシーポリシーをアプリ上に表示し、個人情報を取得する前にあらかじめ利用目的を本人に明示した。
- その際、プライバシーポリシー画面を最後までスクロールするとはじめて「同意する」ボタンが表示される仕様とすることにより、プライバシーポリシーの全体が確実にユーザに対して表示される状態を作り出し、ユーザが内容を確認する機会を提供した上で、同意を得た。
- 生活支援モデル（和歌山）では、ユーザの年齢層が高く、スマートフォンの操作に不慣れなユーザも多く存在した。また、ユーザの居住地域も限定されていたため、アプリのインストールや使用方法を説明する会を開催し、紙の資料を用いて、個人データの利用目的がユーザに認識されるように、対面にて 1 人ずつ丁寧に説明した。このように、ユーザの特性や事業の運営環境等に応じて柔軟な対応をとった。

4.8.3 個人データの管理

取得した個人データの管理に関して、今回のモデル事業の対応状況、及び本書での取扱いは以下の通りである。

図表 67　個人情報保護法（個人データの管理）

No	取得した個人データの管理に関連する事項	モデル事業での対応	本書での取扱い
①	データ内容の正確性の確保等	●	●
②	安全管理措置	●	●
③	従業者の監督	●	●
④	委託先の監督	－	●

凡例）●：モデル事業での対応有、又は本書での取扱有
－：モデル事業での対応無、又は本書での取扱無

①　データ内容の正確性の確保等

法第 19 条
個人情報取扱事業者は、利用目的の達成に必要な範囲内において、個人データを正確かつ最新の内容に保つとともに、利用する必要がなくなったときは、当該個人データを遅滞なく消去するよう努めなければならない

a. 考慮すべき事項

- 利用目的の達成に必要な範囲内において、個人情報データベース等への個人情報の入力時の照合・確認の手続の整備、誤り等を発見した場合の訂正等の手続の整備、記録事項の更新、保存期間の設定等を行うことにより、データ利活用の主要項目（例えば、住所情報といった利用者属性データを分析のキー項目として使用する場合等）が不正確であることより生じる不利益から本人を守るために、個人データを正確かつ最新の内容に保つよう努めなければならない。
- 決済情報や購買情報を分析等して利活用する場合で、一度分析したデータを再度利用する予定がないときは、分析完了後に、個人データを安全な方法で消去すれば、漏えいリスクの回避にもなる。
- 但し、自社が当事者となる契約に関するデータ等については、税法等に基づき、一定期間の保存が必要な場合もあるので、留意する。
- 尚、金融分野の事業者に適用される「金融分野における個人情報保護に関するガイドライン」においては、金融分野の個人情報取扱事業者は、保有する個人データの利用目的に応じた保存期間（契約終了後一定期間内等）を定め、当該期間を経過した個人データを消去することとされている。

b. 今回のモデル事業における対応

- 個人情報の正確性確保のために、一度登録した個人情報の内容をユーザが確認及び修正可能な機能を用意し、ユーザによる個人情報の修正がなされた場合には、データベース上の個人データにも直接反映されるようにした。
- 利用する必要がなくなった時は、個人データを廃棄した。

② 安全管理措置

本書「5 安全管理措置」を参照されたい。

③ 従業者の監督

法第 21 条 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない

a. 考慮すべき事項

- 従業者（派遣社員等も含む）に個人データを取扱わせるにあたって、法第 20 条に基づく安全管理措置（詳細は本書 5.3、5.4 にて解説）を遵守させるよう、当該従業者に対し必要かつ適切な監督をしなければならない。
- 事業開始時の体制整備だけでなく、継続的なモニタリング、定期的な見直し等が必要である。
- 個人データが漏えい等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の規模及び性質、個人データの取扱状況（取扱う個人データの性質及び量を含む。）等に起因するリスクに応じて、個人データを取扱う従業者に対する教育、研修等の内容及び頻度を充実させるなど、必要かつ適切な措置を講ずることが望ましい。
- なお、金融分野の事業者に適用される「金融分野における個人情報保護に関するガイドライン」においては、金融分野の個人情報取扱事業者に、次のような体制整備等を求めているが、金融分野以外の個人情報取扱事業者にも有用な方法である。

  ① 従業者が、在職中及び退職後に、業務に関して知り得た個人データを第三者に知らせ、又は利用目的外に使用しないことを内容とする契約等を採用時等に締結すること。

  ② 個人データの適正な取扱いのための取扱規程の策定を通じた従業者の役割・責任の明確化及び従業者への安全管理義務の周知徹底、教育及び訓練を行うこと。

  ③ 従業者による個人データの持出し等を防ぐため、社内での安全管理措置に定めた事項の遵守状況等の確認及び従業者における個人データの保護に対する点検及び監査制度を整備すること。

b. 今回のモデル事業における対応

- 個人情報を取扱う作業を行う場合の手順書が法第 20 条に基づく安全管理措置を遵守するものであることを品質管理部署で承認するとともに、個人情報を取扱う際には監督者の確認のもと実施した。

- 個人情報を取扱う上での社内ルール及び漏えいした場合の影響について従業者に研修を受けさせた。
- 本書 5.3.4③「安全管理措置の周知徹底、教育及び訓練」の中で定義している定期的な教育コンテンツの受講と理解度確認テストについて、予定通り研修の受講ができていること、及びテストの点数が問題ないことを監督者がチェックした。
- 今回は、事業の実施期間及び地域を限定していること、また要配慮個人情報を扱っていないことから、教育等については、既に整備されている社内研修を受講することで充足すると判断した。
- 従業者が社内ルールを守っていることを監督するため、従業者には毎月自主点検をさせ、監督者がその結果を確認した。

④ 委託先の監督

> 法第 22 条
> 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

a. 考慮すべき事項

- 監督の手段は、取扱いを委託する個人データのプライバシー性の程度、データ量の多寡等に応じて、どこまで厳格にするか検討する。
- 適切な安全管理措置を実施できる委託先を選定する必要があり、特に厳格な取扱いが必要な場合には、P マークや ISMS 等の認証を取得しているかも、1 つの指標として考慮されるケースもある。認証まで必要でない場合であっても、事前に、委託先候補における個人情報保護に関する体制（組織体制、関連規程の整備状況、研修や定期検査の実施状況等）を確認することが望ましい。
- 委託期間中は、定期的又は随時に、報告の要求や場合によっては委託先の事業所への立入検査等が必要になることを想定し、こうした手段を実行可能にするために、具体的な方法等を委託契約等において明確にしておくのが望ましい。
- 特に、平常時に行うべき対応と漏えい事故の発生等の緊急時に行うべき対応について、それぞれの観点から定めておくことも有用である。
- 委託先には、仮名化等した上で情報を受け渡せば、漏えい時のリスク低減につながるため、有用な方法である。この場合、委託先では特定の個人を識別できない状態となっており、委託先単体で見れば個人情報に該当しないとしても、委託元では（他の情報と容易に照合して識別可能な状態等であれば）個人情報である。委託先が扱うのは、あくまで委託元の個人情報であるため、契約上、個人情報としての安全管理措置等を行うように明確に義務付けるべきである。

- 個人データをクラウド上で管理する場合、クラウド事業者による個人データの取扱い状況等によっては、クラウド事業者が委託先に該当する可能性があるため、注意が必要である。

b. 今回のモデル事業における対応

- 今回のモデル事業では、個人データの取扱いの全部又は一部を委託する事案は生じていない。

4.8.4 個人データの第三者への提供

個人データの第三者への提供に関して、今回のモデル事業での対応状況、及び本書での取扱いは以下の通りである。

図表 68　個人情報保護法（個人データの第三者への提供）

No	個人データの第三者への提供に関連する事項	モデル事業での対応	本書での取扱い
①	第三者提供の制限の原則	－	●
②	オプトアウトによる第三者提供	－	●
③	第三者に該当しない場合	●	●
－	外国にある第三者への提供の制限	－	－
－	第三者提供に係る記録の作成等	－	－
④	第三者提供を受ける際の確認等	－	●

凡例）●：モデル事業での対応有、又は本書での取扱有
－：モデル事業での対応無、又は本書での取扱無

①　第三者提供の制限の原則

法第 23 条第 1 項
個人情報取扱事業者は、次に掲げる場合を除くほか、あらかじめ本人の同意を得ないで、個人データを第三者に提供してはならない。

(1) 法令に基づく場合
(2) 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。
(3) 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。
(4) 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

a. 考慮すべき事項

- 同意取得の方式に法令上の制限はないが、同意書への署名・押印等やウェブサイトやアプリ上での同意ボタンのクリック等、記録が残る方式が望ましい。

- 同意取得にあたり、第三者提供する個人データの項目を特定することは必須ではないが、提供される内容がある程度明らかになっている方が、本人の理解を得やすく、個人情報保護の観点からも望ましい。
- 同意取得にあたり、提供先の氏名又は名称を本人に明示することまでは必須ではないが、想定される提供先の範囲や属性を示すことが望ましい。
- 第三者に提供された後の個人データの取扱いについては、基本的に当該第三者の責任となる。しかし、提供先の第三者による取扱いが杜撰であったり本人の想定外の範囲に及んだりするような場合には、提供元の信用にも関わるため、当該第三者との間の契約等において、提供後の個人データの取扱い等について、定めておくことも考えられる。
- 例えば、第三者提供後の提供先における利用目的は、提供元が定める利用目的には制限されないため、個人情報保護により配慮するのであれば、提供先との契約において、あらかじめ利用可能な範囲を定めておくことも考えられる。

b. 今回のモデル事業における対応

今回のモデル事業では、個人データの受け渡しは共同利用として実施し、共同利用者以外にデータ利活用に用いるデータを受け渡す場合は個人データに該当しない統計情報に加工しており、個人データの第三者提供は実施しなかった。

② オプトアウトによる第三者提供

法第 23 条第 2 項
個人情報取扱事業者は、第三者に提供される個人データ（要配慮個人情報を除く。以下この項において同じ。）について、本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止することとしている場合であって、次に掲げる事項について、個人情報保護委員会規則で定めるところにより、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置くとともに、個人情報保護委員会に届け出たときは、前項の規定にかかわらず、当該個人データを第三者に提供することができる。
(1) 第三者への提供を利用目的とすること。
(2) 第三者に提供される個人データの項目
(3) 第三者への提供の方法
(4) 本人の求めに応じて当該本人が識別される個人データの第三者への提供を停止すること。
(5) 本人の求めを受け付ける方法

a. 考慮すべき事項

- オプトアウト手続は、本人の同意取得という原則から外れるという点で、相対的には、個人情報保護の程度が下がるものであり、個人情報保護委員会への届出が求められ、要配慮個人情報には適用できない等、規制は強化される傾向にある。（オプトアウトにより取得した個人データを更にオプトアウトにより提供することも制限される法改正もされている。）
- そのため、第三者提供については、原則通り同意の下で行うのが最も無難な方法といえ、オプトアウト手続を活用するかは、データのプライバシー性の高さ、本人の同意取得の難易度・煩雑度、ユーザが受ける印象等も踏まえて、慎重に検討すべきである。特に、同意取得が困難な事情があって現実的でない局面では、オプトアウト等の活用も検討することになると考えられる。

b. 今回のモデル事業における対応

オプトアウトによる第三者提供は行わなかった。

③ 第三者に該当しない場合

法第 23 条第 5 項
次に掲げる場合において、当該個人データの提供を受ける者は、前各項の規定の適用については、第三者に該当しないものとする。

(1) 個人情報取扱事業者が利用目的の達成に必要な範囲内において個人データの取扱いの全部又は一部を委託することに伴って当該個人データが提供される場合
(2) 合併その他の事由による事業の承継に伴って個人データが提供される場合
(3) 特定の者との間で共同して利用される個人データが当該特定の者に提供される場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

a. 考慮すべき事項

委託

- 委託に伴って個人データを提供する場合、委託先は委託元から受託した業務の範囲内で個人データを取扱う必要があり、委託先が自己又は第三者の事業に転用したり、他の委託元から受領した個人データと混在させて取扱ったりするような場合には、委託の範囲内とは言えない。
- クラウドサービスの利用と委託との関係、及び委託先に対する監督については、「4.8.3④ 委託先の監督」参照。

共同利用

- 複数の事業者にまたがって個人データを利用する方法としては、共同利用の他、同意に基づく第三者提供、共同で取得する方法等があり、同意取得の容易性、事業の枠組み、利用の実態等に応じて最適な方法を選択する。
- 既に特定の事業者が取得している個人データを他の事業者と共同して利用する場合、社会通念上、共同して利用する者の範囲や利用目的等が当該個人データの本人が通常予期し得ると客観的に認められる範囲内である必要がある。
- 上記の場合、既に取得している事業者が取得の際に特定した利用目的の範囲で共同利用しなければならない。
- 共同利用する者の範囲の限界については、客観的な基準はないが、ある程度一体として捉えられる範囲（例えば、グループ企業内や特定の共同事業を行う企業等）であることを前提とした制度であるため、それを逸脱する場合、直ちに違法とまで言えなくても、レピュテーション（評判）リスクが生じる可能性もある。
- 共同利用する者の範囲は、必ずしも固有名詞で列挙する必要まではないが、将来を含め利用される事業者の範囲を本人が判断できる程度である必要があり、例えば、ウェブサイト上に対象となる事業者を掲載し、その範囲内で随時更新する事例も見られる。
- 尚、金融分野の事業者に適用される「金融分野における個人情報保護に関するガイドライン」においては、共同利用する事業者を個別に列挙することが望ましく、その外延のみを示す場合は、本人が容易に理解できるよう具体的に特定する必要があるとされている。
- 共同利用と類似する状態を生み出す仕組みとして、複数の企業等が共同で個人情報を取得するケースがあるが、そのような場合には、各社の利用目的をそれぞれ明示する等して、共同で取得する旨を明らかにする必要がある。

b. 今回のモデル事業における対応

- 今回のモデル事業では、個人データの取扱いの全部又は一部を委託する事案は生じていない。
- 一方、個人データの提供は、共同利用として実施した。そのため、観光支援モデル（埼玉）ではプライバシーポリシーに以下の共同利用の条件を記載した。ホームページ上に継続的に掲載することで、ユーザがいつでもプライバシーポリシーの記載内容を確認できる状態にし、「本人が容易に知り得る状態に置く」という要件を満たした。
- 共同利用者の範囲の記載にあたっては、共同利用する事業者が将来も増えないことが明確であったため、共同利用される範囲が本人にとってより分かりやすくなるよう、具体的な事業者名を記載した。

３．共同利用について
ユーザの個人情報につきまして、以下のとおり共同利用させていただくことがあります。

(1)共同利用する個人情報の項目
氏名、性別、生年月日、郵便番号、秩父観光でやりたいこと、秩父観光への同行者との関係、予定移動手段、メールアドレス、その他連絡先に関する情報等
（本書では、以下省略）

(2)共同利用者の範囲
- 商工会議所名
- データ分析会社名

(3)共同利用の目的
共同利用の目的は、本文書１．(3)に記載された利用目的と同じです（但し、共同利用の利用目的については、「当社」を「当社および共同利用者の範囲に指定する各社」と、また、「本サービス」を「当社および共同利用者の範囲に指定する各社が提供するサービス」と読み替えるものとします）。

(4)個人情報の管理について責任を有する者の名称
・システム開発会社名

④ 第三者提供を受ける際の確認等

法第 26 条第 1 項
個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、次に掲げる事項の確認を行わなければならない。ただし、当該個人データの提供が第 23 条第 1 項各号又は第 5 項各号のいずれかに該当する場合は、この限りでない。
(1) 当該第三者の氏名又は名称及び住所並びに法人にあっては、その代表者（法人でない団体で代表者又は管理人の定めのあるものにあっては、その代表者又は管理人）の氏名
(2) 当該第三者による当該個人データの取得の経緯

第 2 項
前項の第三者は、個人情報取扱事業者が同項の規定による確認を行う場合において、当該個人情報取扱事業者に対して、当該確認に係る事項を偽ってはならない。

a. 考慮すべき事項

- 本人からの委託等に基づき「本人に代わって」第三者提供すると解釈できる場合等、解釈上、確認義務が不要とされることもあるため、ビジネスの設計段階で留意する。
- 「取得の経緯」の具体的な内容は、個人データの内容、第三者提供の態様などにより異なり得るが、基本的には、取得先の別（顧客としての本人、従業員としての本人、他の個人情報取扱事業者、家族・友人等の私人、いわゆる公開情報等）、取得行為の態様（本人から直接取得したか、有償で取得したか、いわゆる公開情報から取得したか、紹介により取得したか、私人として取得したものか等）などを確認しなければならない。
- 仮に、適法に入手されたものではないと疑われるにもかかわらず、あえて個人データの提供を受けた場合には、法第 17 条第 1 項違反と判断される可能性がある。
- 第三者提供を受ける際の確認等については、「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）[48]」も参照。

b. 今回のモデル事業における対応

個人データの第三者提供を受けていないため、これらの確認作業は発生しなかった。

4.8.5 保有個人データに関する事項の公表等、保有個人データの開示、訂正、利用停止等

保有個人データに関連して、今回のモデル事業での対応状況及び本書での取扱いは以下の通りである。

図表 69　個人情報保護法（保有個人データに関する事項）

No	保有個人データに関連する事項	モデル事業での対応	本書での取扱い
①	保有個人データに関する事項の公表等	●	●
②	保有個人データの開示	●	●
③	保有個人データの訂正等	●	－
④	保有個人データの利用停止等	●	－
⑤	理由の説明	●	－
⑥	開示等の請求等に応じる手続き	●	－
－	手数料	－	－
－	裁判上の訴えの事前請求	－	－

凡例）●：モデル事業での対応有、又は本書での取扱有
－：モデル事業での対応無、又は本書での取扱無

[48] 「個人情報の保護に関する法律についてのガイドライン（第三者提供時の確認・記録義務編）」（平成 28 年 11 月公表）参照 URL：https://www.ppc.go.jp/files/pdf/guidelines03.pdf

① 保有個人データに関する事項の公表等

法第 27 条第 1 項
個人情報取扱事業者は、保有個人データに関し、次に掲げる事項について、本人の知り得る状態（本人の求めに応じて遅滞なく回答する場合を含む。）に置かなければならない。

(1) 当該個人情報取扱事業者の氏名又は名称
(2) 全ての保有個人データの利用目的（第 18 条第 4 項第 1 号から第 3 号までに該当する場合を除く。）
(3) 次項の規定による求め又は次条第 1 項、第 29 条第 1 項若しくは第 30 条第 1 項若しくは第 3 項の規定による請求に応じる手続（第 33 条第 2 項の規定により手数料の額を定めたときは、その手数料の額を含む。）
(4) 前三号に掲げるもののほか、保有個人データの適正な取扱いの確保に関し必要な事項として政令で定めるもの

政令第 8 条
法第 27 条第 1 項第 4 号の政令で定めるものは、次に掲げるものとする。
(1) 当該個人情報取扱事業者が行う保有個人データの取扱いに関する苦情の申出先
(2) 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者である場合にあっては、当該認定個人情報保護団体の名称及び苦情の解決の申出先

a. 考慮すべき事項

- 具体的な手段としては、ホームページへの掲載、書面の配布等が考えられるが、氏名・名称、利用目的、苦情の申出先・問い合わせ先等は、プライバシーポリシー等に記載して、ホームページ等に掲載している事例が多く見られる。
- 開示等の請求手続については、上記の事項に比べると情報量が多くなる傾向にあることもあり、ホームページ等に掲載する方法の他、問い合わせがあった際に遅滞なく回答できるように、書面等を用意している事例も多く見られる。

b. 今回のモデル事業における対応

- 各地域のモデル事業では、それぞれの地域ウォレット内にお問い合わせ先の電話番号を記載したページを用意した。またプライバシーポリシーに、当該個人情報取扱事業者の名称や個人情報の利用目的、訂正等の請求に応じる手続、問い合わせ先等について、記載している。

＜個人情報保護管理者および個人情報保護担当者＞
・個人情報保護管理者：　システム開発会社　XX 部　本部長
・個人情報保護担当者：　システム開発会社　XX 部　氏名

＜個人情報の開示、訂正・削除等について＞
ご記入いただいたご自身の個人情報の開示、訂正・削除等をご希望される場合は、法令等に従い、遅滞なく対応させていただきます。
また、個人情報の開示、訂正・削除等をご希望される場合または個人情報の取扱いに関しご質問やご不明なところがある場合、お問い合わせ先までご遠慮なくお申しつけくださいますようお願いします。
なお、ユーザはいつでもご登録されているメールアドレスやパスワード等の情報を、本アプリ上で確認、訂正することができます。
ユーザから当社への個人情報の提供は任意ですが、必要な情報を提供いただけない場合、本サービスの一部または全部を利用できない場合がございます。

＜お問い合わせ＞
本文書に関してご不明な点がある場合、本サービスにおける個人情報の取扱いに関するご質問・苦情・ご相談等があります場合は、本アプリ内のお問い合わせリンクよりご連絡ください。

- 当該個人情報取扱事業者が認定個人情報保護団体の対象事業者であったため、自社のウェブサイトに掲示する方法により、当該認定個人情報保護団体の名称及び苦情の解決の申出先を予め公表した。

＜認定個人情報保護団体について＞
「認定個人情報保護団体」の名称及び苦情の解決の申出先

認定個人情報保護団体の名称
　一般財団法人日本情報経済社会推進協会
苦情の解決の申出先
　個人情報保護苦情相談室
住所
　〒xxx-xxxx
　東京都港区六本木一丁目ＸＸＸ
電話番号
　03-xxxx-xxxx
　0120-xxx-xxx（フリーダイヤル）
※当社の商品・サービスに関する問合せ先ではございません。

② 保有個人データの開示

法第 28 条
1 本人は、個人情報取扱事業者に対し、当該本人が識別される保有個人データの開示を請求することができる。
2 個人情報取扱事業者は、前項の規定による請求を受けたときは、本人に対し、政令で定める方法により、遅滞なく、当該保有個人データを開示しなければならない。ただし、開示することにより次の各号のいずれかに該当する場合は、その全部又は一部を開示しないことができる。
(1) 本人又は第三者の生命、身体、財産その他の権利利益を害するおそれがある場合
(2) 当該個人情報取扱事業者の業務の適正な実施に著しい支障を及ぼすおそれがある場合
(3) 他の法令に違反することとなる場合
3 個人情報取扱事業者は、第 1 項の規定による請求に係る保有個人データの全部又は一部について開示しない旨の決定をしたとき又は当該保有個人データが存在しないときは、本人に対し、遅滞なく、その旨を通知しなければならない。
4 他の法令の規定により、本人に対し第 2 項本文に規定する方法に相当する方法により当該本人が識別される保有個人データの全部又は一部を開示することとされている場合には、当該全部又は一部の保有個人データについては、第 1 項及び第 2 項の規定は、適用しない。

a. 考慮すべき事項

- 本人から、当該本人が識別される保有個人データの開示の請求を受けたときは、本人に対し、書面の交付による方法（開示の請求を行った者が同意した方法があるときはその方法）[49] により、遅滞なく、当該保有個人データを開示しなければならない。
- 本項で触れた開示請求のほか、本人から、当該本人が識別される保有個人データについて、当該保有個人データの内容の訂正、追加若しくは削除又は利用の停止若しくは消去の請求を受けた場合であって、その請求に理由があるときは、原則として、遅滞なく対応しなければならないことにも留意すべきである。

b. 今回のモデル事業における対応

- 問合わせにより個人データの開示請求があった場合には、書面による交付を滞りなく行うこととした。
- 個人データの内容の訂正や削除等の請求があった場合には、遅延なく対応することとした。

[49] 令和 2 年改正法では、電磁的記録の提供を含め、本人が方法を指定できるようになる
個人情報保護委員会「改正個人情報保護法 政令・規則・ガイドライン等の整備に当たっての基本的な考え方について」
参照 URL：https://www.ppc.go.jp/files/pdf/200722_kihontekikangae.pdf

4.8.6 その他

① 仮名加工情報について

仮名加工情報とは、令和 2 年改正法の施行をもって適用される概念であり、他の情報と照合しない限り特定の個人を識別することができないように個人情報を加工したデータのことをいう[50] 。（2.4.1①）参照）

今回のモデル事業では、共同利用者にデータを渡す際に以下のように仮名加工を実施した。

図表 70 個人情報保護法（今回のモデル事業での仮名加工方法例）

No.	項目	個人データサンプル	仮名加工データサンプル
1	携帯電話番号	9012345678	2087594125
2	ログインパスワード	Efievn3242	連携しない
3	メールアドレス	sample@abc.co.jp	****
4	取引暗証番号	123456	連携しない
5	氏名（姓）	会津	****
6	氏名（名）	太郎	****
7	性別	0＝ 不明、1=男性、2＝女性	0, 1, 2
8	生年月日	20020711	2002
9	郵便番号	1601245	1601245
10	住所	東京都新宿区西新宿３丁目２－１	****
11	目的地	元中山 1-11-11	元中山 1-11-11
12	高速バス乗車日時	1909	1909
13	乗車人数	3	3
14	ご連絡先	sample@abc.co.jp	****
15	同居人数	2	2
16	ポイントカード ID	0000-00-0000000000	****

仮名加工する上での考慮点としては、次のようなものが挙げられる。

- データ利活用のための分析に影響ない範囲で情報を加工する。
  具体的には、氏名は分析には不要のためマスキングを行う。生年月日は生まれた年のみの情報に加工し、住所は郵便番号で取得できる情報に加工する。

[50] 仮名加工情報の部分のみが委託、共同利用によって提供される場合、提供先において容易照合性がなければ、提供先にとっては個人情報ではない仮名加工情報となる。

② 統計情報への加工について

統計情報は、複数人の情報から共通要素に係る項目を抽出して同じ分類ごとに集計して得られるデータであり、集団の傾向又は性質等を数量的に把握するものである。したがって、統計情報は特定の個人との対応関係が排斥されている限りにおいては、法における「個人に関する情報」に該当するものではない。

注意点

ある分類においてサンプルが 1 つしか存在しない場合、特定の個人に該当する可能性があるため、データから削除する等の対応が必要となる。

5 安全管理措置

本章では、データ利活用推進主体、データ利活用基盤システム運用者、データ分析者にあたる各関連事業者が、適切な安全管理措置を取れるように、データ利活用基盤を運営する際の安全管理措置について説明する。

法第 20 条
個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

5.1 安全管理措置について

各関連事業者は、データ利活用において取扱う個人データの漏えい、滅失又は毀損の防止その他の個人データの安全管理のため、安全管理に係る基本方針・取扱規程等の整備、及び安全管理措置に係る実施体制の整備等の必要且つ適切な措置を講じなければならない。必要且つ適切な措置は、個人データの取得・利用・保管等の利活用における各段階に応じた「組織的安全管理措置」、「人的安全管理措置」、「物理的安全管理措置」、及び「技術的安全管理措置」を含むものでなければならない。

また、必要且つ適切な措置の他方で、当該措置は個人データが漏えい、滅失又は毀損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質、個人データの取扱状況及び、データ利活用の性質等に起因するリスクに応じたものとする。

尚、安全管理措置の基本的な内容については、それぞれの事業者等に適用される各省庁管轄のガイドラインに従うこと。今回は本書の想定読者である 3 つのロール（データ利活用推進主体、データ利活用基盤システム運用者、データ分析者）に対して大きく 2 パターンの安全管理措置を用意している。

まず、主たる読者として決済事業者と接続するデータ利活用基盤システム運用者を想定した「5.3 安全管理措置の内容」では、「金融分野における個人情報保護法に関するガイドライン」[51]、及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」[52]を拠りどころとした[53]。

---

[51] 金融分野における個人情報保護に関するガイドライン（平成 29 年 2 月 28 日個人情報保護委員会・金融庁告示第 1 号（平成 29 年 5 月 30 日施行））
参照 URL：https://www.fsa.go.jp/common/law/kj-hogo-2/01.pdf

[52] 金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針（平成 29 年 2 月 28 日個人情報保護委員会・金融庁告示第 2 号（平成 29 年 5 月 30 日施行））
参照 URL：https://www.fsa.go.jp/common/law/kj-hogo-2/03.pdf

[53] この他に、具体的な事例を本書で記載するにあたり、「（別添）特定個人情報に関する安全管理措置（事業者編）」も参照した。

そして、主たる読者としてデータ利活用推進主体及び、データ分析者を想定した「5.4 安全管理措置の内容（データ利活用推進主体及び、データ分析者向け）」では、「個人情報の保護に関する法律についてのガイドライン(通則編)」の（別添）講ずべき安全管理措置の内容を拠りどころとした。

尚、前者の金融分野のガイドラインは、後者の通則編と比してより厳格な安全管理措置を求める内容となっている。

「5.3　安全管理措置の内容」が対象とするデータ利活用基盤システム運用者とは、図表 1.5-01「データ利活用におけるロールと想定される各関連事業者」に記載の通り、「データ利活用基盤を提供し、データ保持、及び加工をする事業者等」の役割を担うものであり下記の特徴がある。

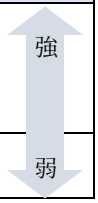
- 決済事業者と接続している。
- 決済データや個人データ等の生データを持っている。
- 地域ウォレットアプリを運用している。

事業者によっては金融分野のガイドラインが直接的に適用されない場合も想定されるが、そうした場合であっても、決済データ等を扱うようなときには、金融分野のガイドラインに準じることが望ましいことより、データ利活用基盤システム運用者に該当する読者は 5.3 節を参照されたい。

「5.4　安全管理措置の内容（データ利活用推進主体及び、データ分析者向け）」が対象とする「データ利活用推進主体」、及び「データ分析者」は、上述のデータ利活用基盤システム運用者の特徴には該当せず、主にデータ加工されてリスクが低い状態のデータを扱う事業者であると想定している。そのため、5.4 節では最も基礎的な通則編に準じることとしている。

図表 71　参考にする目次とその読者

想定読者	対象の目次	参照先ガイドライン	求められる安全管理措置の強度
データ利活用基盤システム運用者	5.3 節	「金融分野における個人情報保護法に関するガイドライン」 、及び「金融分野における個人情報保護に関するガイドラインの安全管理措置等についての実務指針」	強化事例 基本事例
データ利活用推進主体、データ分析者	5.4 節	「個人情報の保護に関する法律についてのガイドライン(通則編)」	基礎編



参照 URL：https://www.ppc.go.jp/files/pdf/my_number_guideline_jigyosha.pdf

5.2 安全管理措置の検討手順

データ利活用推進主体等は、データ利活用におけるデータの取扱いを検討するに当たり、事業の範囲（4 章におけるステークホルダリストや、ビジネス関係図等での整理内容）、及びデータの範囲（4 章におけるデータリソースマップ、データフローシーケンス等での整理内容）を明確にした上で、個人データを取扱う事業者及び担当者を明確にしておく必要がある。

これらを踏まえ、個人データの適正な取扱いの確保について組織として取り組むために、基本方針や取扱規程等を策定し体制の整備及び情報システムの改修等を次のような手順で検討する。

(1) 個人データの安全管理に関する基本方針の策定
(2) 個人データの安全管理に関する取扱規程等の策定
(3) 実施体制の整備に関する組織的安全管理措置
(4) 実施体制の整備に関する人的安全管理措置
(5) 実施体制の整備に関する物理的安全管理措置
(6) 実施体制の整備に関する技術的安全管理措置

5.3 安全管理措置の内容

本節では、データ利活用基盤システム運用者向けに、個人データ保護のために必要な安全管理措置を記載する。決済データの生データを取扱うデータ利活用基盤システム運用者は、個人データ保護のために必要な安全管理措置について、個人データの安全管理や実施体制の整備等の措置を講じなければならない。

また、安全管理措置の検討・実施にあたり、個人情報保護法等の関連法令、並びに、本書及び個人情報保護法ガイドライン等の遵守のほか、個人データが漏洩、滅失又は毀損等をした場合に本人が被る権利利益の侵害の大きさを考慮し、事業の性質、個人データの取扱状況、及びデータ利活用の性質等に起因するリスクに応じた措置を講ずる。

本章では、安全管理措置を実施する上での対応事項や具体的実施内容等を「手法の例示」で例示する。なお、(5) 実施体制の整備に関する物理的安全管理措置及び、(6) 実施体制の整備に関する技術的安全管理措置については、事業者が取扱う個人データやそのシステム特性に応じて講ずる対策を採用できるよう、「基本事例」と「強化事例」

に分けて対策を例示している。例えば、取扱う個人データの内容や加工の程度によって漏えいしたときに本人が被る被害が小さいと想定できれば、採用する対応は「基本事例」とする場合もある。一方で、データ量が多く、加工されていない個人データ等を取扱うなど、漏えいしたときに本人が被る被害が大きくなると想定できるのであれば「強化事例」を採用する場合もある。これらの採用すべき安全管理措置の検討にあたっては、例えば以下のような考慮要素を検討することが有用であると考えられる。

- 取扱う個人データの量
  取扱う個人データの量が多くなればなるほど、インシデント時の被害が拡大することになる。
- 取扱う個人データの内容
  例えば、取扱う個人データに要配慮個人情報や、「金融分野における個人情報保護法に関するガイドライン」に定める機微（センシティブ情報）が含まれていたり、そうでないとしても、プライバシー性の高い情報が含まれていたり、そのデータを利用することで不正に決済ができてしまう等、不正に利用されることにより財産的被害が生じるおそれがある個人データが含まれる場合には、漏えい時の本人が被る被害が大きくなる。また、一般に、取扱う個人データの項目が増えれば、つまり、個人データがリッチであるほど、同様に、漏えい時の本人が被る被害が大きくなると考えられる。
- 取扱う個人データの加工の程度
  個人データを取扱うとしても、仮名加工したデータしか取扱わないのであれば、漏えいしたときに本人が被る被害が小さいと考えられるが、その加工の程度によって、本人が被る被害が変わりうる。また、当該加工済みのデータと一般に入手できるデータとを照合することにより復元し、本人を特定することが容易であるかどうかも考慮すべきである。
- 個人データを記録した媒体の性質
  不特定多数の人からアクセス可能な状態であれば、それだけ漏えいするリスクが高まり、データへのアクセスが限定的であればあるほど、そのリスクは低くなる。またデータの保存期間が短ければ、その分だけ漏えいする確率も下がることが考えられる。

また、今回のモデル事業では決済事業者との接続等もありセキュリティ面を重視したため、「強化事例」に近い状態で安全管理措置を講じた。データ利活用基盤システム運用者が実施した対応内容を、「今回のモデル事業での具体例」にて例示する。本例示

はこれに限定する趣旨で記載したものではなく、上記のような要素等を検討の上、事業者自身が適切な手法を判断し採用することが重要である。

5.3.1 個人データの安全管理に関する基本方針の策定

データ利活用基盤システム運用者等は、データ利活用における個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定し、当該基本方針を公表するとともに、必要に応じて見直しを行わなければならない。

① 手法の例示

基本方針に定める項目としては、次に掲げるものが挙げられる。

- 事業者の名称
- 個人データの安全管理措置に関する宣言
- 基本方針の継続的改善の宣言
- 関連法令・ガイドライン等の遵守に関する宣言
- 質問及び苦情処理の窓口

② 今回のモデル事業での具体例

会社として、以下の基本方針をウェブサイト上にて公表している。

当社は、適切な個人情報保護を実施するための基本方針を下記の通り宣言し、JIS 規格（JIS Q 15001:2017）に準拠して定めた個人情報保護に関するマネジメントシステムの実施ならびに改善を行います。

- 事業の内容および規模を考慮した適切な個人情報の取得、利用および提供について定めた社内規定を遵守します。この規定には個人情報の利用目的の達成に必要な範囲を超えた取り扱いを行わないことおよびそのための措置を含みます。
- 個人情報への不正アクセス、個人情報の紛失、破壊、改ざんおよび漏えいなどの予防ならびに是正に関する適切な措置を講じます。
- 個人情報保護に関するマネジメントシステムを継続的に改善します。
- 個人情報に関する法令、国が定める指針やその他の規範を遵守します。
- 個人情報に関する苦情、相談への対応を実施します。

個人情報保護方針に関するお問い合わせ先
システム開発会社　XX 部

201X 年 4 月 1 日 システム開発会社
代表取締役会長兼社長　○○○○

5.3.2 個人データの安全管理に関する取扱規定等の策定

データ利活用基盤システム運用者等は、以下について規定の策定等を実施する必要がある。

① 個人データの安全管理に係る取扱規程の整備
② 個人データの取扱状況の点検及び監査に係る規程の整備
③ 外部委託に係る規程の整備

① 個人データの安全管理に係る取扱規程の整備

データ利活用基盤システム運用者等は、「5.2 安全管理措置の検討手順」にて明確化した、個人データを取扱う事業者、担当者、及び個人データの範囲に基づき、データ利活用の流れを整理し、事業の実施体制の整備や個人データの具体的な取扱いを定める取扱規程等を策定しなければならない。

a. 手法の例示

取扱規程等の策定は、次に掲げる管理段階ごとに、取扱者の役割・責任、取扱者の限定、個人データの安全管理上必要とされる手続きについて定める。また、具体的に定める事項については、次項以降の(3)から(6)に記述する各安全管理措置を織り込むことが重要である。

- 取得段階
- 利用段階
- 保存段階
- 提供段階
- 削除／廃棄段階

b. 今回のモデル事業での具体例

すべての段階において、取扱方法、取扱者の役割・責任、取扱者の限定及び個人データの安全管理上必要とされる手続きについて規定した。

② 個人データの取扱状況の点検及び監査に係る規程の整備

データ利活用基盤システム運用者等は、個人データの取扱状況に関する点検及び監査の規程を整備し、次に掲げる事項を定めるとともに、必要に応じて規程の見直しを行わなければならない。なお、個人データ取扱部署が単一である事業者においては、点検により監査を代替することも認められる。

a. 手法の例示

- 点検及び監査の目的
- 点検及び監査の実施部署
- 点検責任者及び点検担当者の役割・責任
- 監査責任者及び監査担当者の役割・責任
- 点検及び監査に関する手続

b. 今回のモデル事業での具体例

社内規程にて上記事項について定めている。

③ 外部委託に係る規程の整備

データ利活用基盤システム運用者等は、外部委託に係る取扱規程を整備し、次に掲げる事項を定めるとともに、定期的に規程の見直しを行わなければならない。

a. 手法の例示

- 委託先の選定基準
- 委託契約に盛り込むべき安全管理に関する内容

b. 今回のモデル事業での具体例

社内規定にて委託先の選考・審査・管理について定めている。

5.3.3 実施体制の整備に関する組織的安全管理措置

データ利活用基盤システム運用者等は、個人データの適正な取扱いのために、次に掲げる組織的安全管理措置を講じなければならない。

① 個人データの管理責任者等の設置
② 就業規則等における安全管理措置の整備
③ 個人データの安全管理に係る取扱規程に従った運用
④ 個人データの取扱状況を確認できる手段の整備
⑤ 個人データの取扱状況の点検及び監査体制の整備と実施
⑥ 漏洩事案等に対応する体制の整備

① 個人データの管理責任者等の設置

データ利活用基盤システム運用者等は、「個人データの管理責任者等の設置」として、個人データの安全管理に係る業務遂行の総責任者である「個人データ管理責任者」、及び個人データを取扱う各部署等における「個人データ管理者」を設置しなければならない。また、個人データの管理責任者等に次に掲げる業務を所管させなければならない。

a. 手法の提示

A.「個人データ管理責任者」の所管業務

- ✓ 個人データの安全管理に関する規程及び委託先の選定基準の承認及び周知
- ✓ 個人データ管理者及び本人確認に関する情報の管理者の任命
- ✓ 個人データ管理者からの報告徴収及び助言・指導
- ✓ 個人データの安全管理に関する教育・研修の企画
- ✓ その他事業者における個人データの安全管理に関すること

B.「個人データ管理者」の所管業務

- ✓ 個人データの取扱者の指定及び変更等の管理
- ✓ 個人データの利用申請の承認及び記録等の管理
- ✓ 個人データを取扱う保管媒体の設置場所の指定及び変更等
- ✓ 個人データの管理区分及び権限についての設定及び変更の管理
- ✓ 個人データの取扱状況の把握
- ✓ 委託先における個人データの取扱状況等の監督
- ✓ 個人データの安全管理に関する教育・研修の実施
- ✓ 個人データ管理責任者に対する報告
- ✓ その他所管部署等における個人データの安全管理に関すること

b. 今回のモデル事業での具体例

「個人データ管理責任者」を社内に 1 名、「個人データ管理者」をプロジェクト内で 1 名任命して運用した。

② 就業規則等における安全管理措置の整備

データ利活用基盤システム運用者等は、「就業規則等における安全管理措置の整備」として、個人データの取扱いに関する従業者等の役割・責任及び違反時の懲戒処分に関する事項を含む就業規則等を定めるとともに、従業者等との個人データの非開示契約等を締結しなければならない。

a. 手法の提示

- 就業規則等制定と、従業者等との個人データの非開示契約等を締結

b. 今回のモデル事業での具体例

- 上記の通り、従業員等の就業規則を規定した。
- 採用時にデータの非開示契約を締結した。

③　個人データの安全管理に係る取扱規程に従った運用

データ利活用基盤システム運用者等は、「個人データの安全管理に係る取扱規程に従った運用」として、取扱規程等に基づく運用を行うとともに、その状況を確認するため、個人データの利用状況、取扱規程に規定する事項の遵守状況等の記録及び確認を行わなければならない。

a. 手法の例示

記録、確認する項目としては、次に掲げるものが挙げられる。

- 個人データの利用・出力状況の記録
- 書類・媒体等の持ち運びの記録
- 個人データの削除・廃棄記録
- 削除・廃棄を委託した場合、これを証明する記録等
- 個人データを情報システムで取扱う場合、システム利用者の情報システム利用状況の記録

b. 今回のモデル事業での具体例

- 利用記録・持ち運び記録、削除・破棄記録を保存した。
- 削除されたことがわかる証跡を残すことで、削除されたことを証明する記録を保存した。例えば、データ削除専用のソフトウェアを使い取得した削除後画面のスクリーンショット、及び、削除前後のデータ件数が比較できるログを記録として保存した。
- 個人データにアクセスする特定端末及び、そのサーバでの利用履歴の記録を保存した。

④　個人データの取扱状況を確認できる手段の整備

データ利活用基盤システム運用者等は、「個人データの取扱状況を確認できる手段の整備」として、次に掲げる事項を含む台帳等を整備し個人データの取扱状況を確認するための手段を講じなければならない。

- 取得項目
- 利用目的
- 保管場所、保管方法、保管期限
- 管理部署
- アクセス制御の状況

a. 手法の例示

取扱状況を確認するための記録等としては、次に掲げるものが挙げられる。

- 個人情報が含まれるファイルの種類、名称

- 責任者、取扱部署、管理部署
- 取得項目
- 利用目的
- 保管場所、保管方法、保管期限
- 削除、廃棄状況
- アクセス権を有する者
- アクセス制御の状況

b. 今回のモデル事業での具体例

- 上記観点について明記した個人情報保護計画書をプロジェクト・チーム毎に作成した。
- 上記観点以外にも個人データの取扱い全体を把握するのに必要な情報を収集した。（取得する個人情報の人数規模、取得方法、アクセス監視、第三者提供、共同利用、委託があるか等）

⑤　個人データの取扱状況の点検及び監査体制の整備と実施

データ利活用基盤システム運用者等は、「個人データの取扱状況の点検及び監査体制の整備と実施」として、個人データを取扱う部署等が自ら行う点検体制を整備し点検を実施するとともに、当該部署以外の者による監査体制を整備し、監査を実施しなければならない。また、点検、監査の実施にあたり、新たなリスクに対応するための安全管理措置の評価、見直し及び改善に向けて、個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者により実施することが望ましい。

a. 手法の例示

個人データの取扱状況の点検及び監査体制の整備の実施としては、次に掲げるものが挙げられる。

- 点検責任者、及び担当者の選任
- 個人データ取扱部署以外等、独立性のある監査責任者・監査担当者の選任
- 点検／監査計画を策定することにより点検／監査体制を整備し、定期的及び臨時に点検／監査を実施
- 点検／監査終了後に規程違反事項等を把握した時はその改善を実施

b. 今回のモデル事業での具体例

ISMS[54]、PMS[55] の実施体制を確立し、その中で運用した。

⑥ 漏えい事案等に対応する体制の整備

データ利活用基盤システム運用者等は、「漏えい事案等に対応する体制の整備」として、漏えい事案等に対応するため、次に掲げる体制を整備しなければならない。

- 対応部署
- 漏えい事案等の影響・原因等に関する調査体制
- 再発防止策・事後対策の検討体制
- 自社内外への報告体制

また、自組織内外への報告体制を整備するとともに、漏洩事案等が発生した場合には、次に掲げる事項を実施しなければならない。

- 監督当局等への報告
- 本人への通知等
- 二次被害の防止、類似事案の発生回避等の観点からの漏えい事案等の事実関係及び再発防止策等の早急な公表

a. 手法の例示

情報漏えい等の事案の発生時、発生した事案をデータ利活用基盤システム運用者等が正確に把握し、被害拡大防止、復旧、再発防止等を迅速且つ的確に行うことを可能にするための機能を有する体制となる CSIRT[56]や、次に掲げる体制を整備することが考えられる。

- 事実関係の調査及び原因の究明
- 影響を受ける可能性のある本人への連絡
- 個人情報保護委員会又は事業所管大臣等への報告
- 再発防止策の検討及び決定
- 事実関係及び再発防止策等の公表

---

[54] 「ISMS」とは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。参照 URL: https://isms.jp/isms/

[55] 「PMS」とは、個人情報保護マネジメントシステムの略で、「個人情報」を安全に管理する体制を整え、継続的に改善するための管理の仕組みのことを指す。
参照 URL：https://privacymark.jp/wakaru/kouza/theme3_02.html

[56] 「CSIRT」とは、コンピュータやネットワーク（特にインターネット）上で何らかの問 題（主にセキュリティ上の問題）が起きていないかどうか監視すると共に、万が一問題が発生した場合にその原因解析や影響範囲の調査等を行う組織の総称。
参照 URL：https://www.soumu.go.jp/main_content/000727474.pdf

b. 今回のモデル事業での具体例

セキュリティインシデント発生時のフローを定義した。

※セキュリティインシデントとは、不正アクセス、漏えい、改ざん、誤配送、情報資産端末の紛失等を含む。

フローは以下について定義をした。

- セキュリティインシデントレベルに応じた対策本部の設置及び、対外的な対応
- 発見者及び、その上長の具体的な行動
- 原因の究明及び、組織としての再発防止策の検討

5.3.4 実施体制の整備に関する人的安全管理措置

個人データの安全管理措置に係る実施体制の整備における人的安全管理措置として、従業員との間で次に掲げる措置を講じなければならない。

① 個人データの非開示契約等の締結
② 役割・責任等の明確化
③ 安全管理措置の周知徹底、教育及び訓練
④ 個人データ管理手続の遵守状況の確認

① 個人データの非開示契約等の締結

データ利活用基盤システム運用者等は、「個人データの非開示契約等の締結」として、採用時等に従業者と個人データの非開示契約等を締結するとともに、非開示契約等に違反した場合の懲戒処分を定めた就業規則等を整備しなければならない。

a. 手法の例示

- 就業規則等制定と、従業者等との個人データの非開示契約等を締結

b. 今回のモデル事業での具体例

- 採用時にデータの非開示契約を締結した。
- 懲戒処分を定めた就業規則等を整備した。

② 役割・責任等の明確化

データ利活用基盤システム運用者等は、「役割・責任等の明確化」として、次に掲げる措置を講じなければならない。

a. 手法の例示

- 各管理段階における個人データの取扱いに関する従業者の役割・責任の明確化
- 個人データの管理区分及びアクセス権限の設定

- 違反時の懲戒処分を定めた就業規則等の整備
- 必要に応じた規程等の見直し

b. 今回のモデル事業での具体例

個人データ管理者の責任範囲にて、各管理段階の個人データの取扱いを行った。

③ 安全管理措置の周知徹底、教育及び訓練

データ利活用基盤システム運用者等は、「安全管理措置の周知徹底、教育及び訓練」として、次に掲げる措置を講じなければならない。

- 従業者に対する採用時の教育及び定期的な教育・訓練
- 個人データ管理責任者及び個人データ管理者に対する教育・訓練
- 個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知
- 従業者に対する教育・訓練の評価及び定期的な見直し

a. 手法の例示

- 教育及び定期的な教育・訓練の実施と、違反した場合の懲戒処分の周知

b. 今回のモデル事業での具体例

従業者に対して、採用時及び、ある一定期間ごとに、教育コンテンツ（個人データの安全管理に係る就業規則等に違反した場合の懲戒処分の周知も含まれる）の受講及び、理解度を確認するためのテストをセットで実施依頼した。[57]

④ 個人データ管理手続きの遵守状況の確認

データ利活用基盤システム運用者等は、「個人データ管理手続の遵守状況の確認」として、個人データの安全管理に係る取扱規程に定めた事項の遵守状況について、(3) ii に基づく記録及び確認を行うとともに、(3) v に基づき点検及び監査を実施しなければならない。

a. 手法の例示

- 遵守状況について、記録及び確認、点検及び監査の実施

b. 今回のモデル事業での具体例

ISMS、PMS の実施体制を確立し、その中で運用した。

[57] IPA（情報処理推進機構）がセキュリティに関する教育系コンテンツをいくつか用意しているため参考にするとよい。
参照 URL：https://www.ipa.go.jp/security/keihatsu/features.html

5.3.5 実施体制の整備に関する物理的安全管理措置

データ利活用基盤システム運用者等は、個人データの安全管理措置に係る実施体制の整備における「物理的安全管理措置」として、次に掲げる措置を講じなければならない。

① 個人データを取扱う区域の管理
② 機器及び電子媒体等の盗難等の防止
③ 電子媒体等の取扱いにおける漏洩等の防止
④ 個人データの削除、機器及び電子媒体等の廃棄

① 個人データを取扱う区域の管理

データ利活用基盤システム運用者等は、「個人データを取扱う区域の管理」として、情報システム（サーバ等）を管理する区域（以下、管理区域という）を明確にし、物理的な安全管理措置を講ずる。また、個人データを取扱う事務を実施する区域（以下、取扱区域という）について、個人情報取扱担当者等以外の者が個人データを容易に閲覧等できないよう留意する必要がある。

a. 手法の例示

個人データを取扱う区域の管理としては、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
管理区域の定義	管理区域へ入室できるシステム利用者を制限し、IC カード又は生体認証等により入退室を制御する。 守衛や防犯カメラを設置し、監視する。	基本事例に加え、入室ログのない退室は、許可しない。 インターロック（二重扉）を実施する。 管理区域へ持ち込む機器等（携帯電話や録画機器等）の制限をする。
取扱区域の定義	業務・プロジェクト単位に、ついたて等で仕切りを作り周りから中の様子を見えなくする。	業務・プロジェクト単位に部屋を分けて作業する。 取扱区域へ入室できるシステム利用者を制限し、IC カード又は生体認証等により入退室を制御する。 取扱区域へ持ち込む機器等（携帯電話や録画機器等）の制限をする。
入退室管理	オフィスや部屋の入退出時を、社員証等の ID で管理する。 帰宅時には、オフィスや部屋を鍵で施錠する。	常時、IC カード又は生体認証等により、各区域の入退室を記録・制限する。 守衛や防犯カメラを設置する。

b. 今回のモデル事業での具体例

- データセンターに管理区域を用意し、情報システム（サーバ等）を設置した。
- 執務室エリア内に取扱区域（ビデオ監視機能による物理アクセスの監視、入退室者のログ情報の取得・追跡、外部からのぞき込み防止等が可能な設備を有する）を用意した。
- 取扱区域には同行者の付き添いを必須とし、入退室できる権限を必要最低限の担当者にのみ設定した。

② 機器及び電子媒体等の盗難等の防止

データ利活用基盤システム運用者等は、「機器及び電子媒体等の盗難等の防止」として、管理区域及び取扱区域における個人データを取扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、物理的な安全管理措置を講ずる。

a. 手法の例示

機器及び電子媒体等の盗難等の防止としては、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
情報機器の持ち出し防止	・情報システムへアクセスできる端末機器（以下「アクセス機器」という）をワイヤー等で固定する。 ・情報システム（サーバ等）は、管理区域内の施錠されたサーバラック内に保管する。	基本事例に加え、アクセス機器の設置場所を、アクセス制御された区域内にし、入退出の記録をとる。[58]
情報機器の設置場所の監視	情報機器等の情報資産の棚卸しを定期的に行う。	基本事例に加え、 情報機器の設置場所や入口付近に監視カメラを置く等、不正な侵入を監視する。 外部からの不正な侵入に対して警報を鳴らす。

b. 今回のモデル事業での具体例

上記「強化事例」と同様のレベルにて運用した。

[58] 強化事例は、前項「i.個人データを取扱う区域の管理」に記載されている取扱区域に設置するアクセス機器の内容となる。管理区域に設置する機器(サーバー等)については、既にアクセス制御されている区域となるため、持ち出し防止は管理区域内で行う基本事例以上のことはない。

③　電子媒体等の取扱いにおける漏えい等の防止

データ利活用基盤システム運用者等は、「電子媒体等の取扱いにおける漏えい等の防止」として、個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易にデータ内容等が判明しないよう、安全な方策を講ずる。

a. 手法の例示

電子媒体等の取扱いにおける漏えい等の防止としては、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
電子媒体の持ち運び	持ち運ぶデータにパスワードを設定する。 持ち帰り後、データを消去する。	持ち運ぶデータの暗号化、パスワードによる保護、施錠できる搬送容器の使用、追跡可能な移送手段を利用する。
書類等の持ち運び	データ利活用に関連する業務においては個人データが記載された書類の持ち運びはしない。電子媒体での取扱いに留める。	なし

b. 今回のモデル事業での具体例

個人データの入った電子媒体は取扱区域内での持ち運びが発生し、基本事例に則り実施した。書類等を持ち運ぶは実施していない。

④　個人データの削除、機器及び電子媒体等の廃棄

データ利活用基盤システム運用者等は、「個人データの削除、機器及び電子媒体等の破棄」として、個人データの利用や保管等の必要がなくなった場合で、且つ所管法令等において定められている保存期間等を経過した場合には、個人データをできるだけ速やかに復元不可能な手段で削除又は廃棄する。また、個人データを削除した場合、又は電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存する。これらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて、証明書等により確認する。

a. 手法の例示

個人データの削除、機器及び電子媒体等の廃棄としては、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
書類等の廃棄	シュレッダーを利用する等、容易に復元できない手段を採用する。	焼却又は溶解、復元不可能な程度に細断可能なシュレッダーの利用等、復元不可能な手段を採用する。

観点	基本事例	強化事例
機器及び電子媒体等の廃棄	専用のデータ削除ソフトウェアの利用又は物理的な破壊等の手段を採用する。	基本事例に加え、廃棄証明書を履歴として保管する。
データ削除	容易に復元できない手段を採用する。	ログやバックアップのデータも含めて、復元不可能な手段を採用し削除する。 ハードディスクのデータ消去においては、ゼロ埋めや乱数等で複数回データを書き替える。
保存期間経過後のデータ削除	保存期間経過後における廃棄を前提とした情報システム構築及び手続きを定める。	基本事例に加え、保存期間経過後に自動でログを削除する機能を構築する。

b. 今回のモデル事業での具体例

- 復元不可能な手段を採用してデータを削除した。
- データ削除後も安定稼働可能な設計・構築をした。
- あらかじめデータを破棄する期日を設定した。

5.3.6 実施体制の整備に関する技術的安全管理措置

データ利活用基盤システム運用者等は、個人データの安全管理措置に係る実施体制の整備における「技術的安全管理措置」として、次に掲げる措置を講じなければならない。

① 個人情報取扱担当者の識別及び認証
② 個人データの管理区分の設定及びアクセス制御
③ 個人データへのアクセス権限の管理
④ 個人データの漏洩・毀損等防止策
⑤ 個人データへのアクセスの記録及び分析
⑥ 個人データを取扱う情報システムの稼働状況の記録及び分析
⑦ 個人データを取扱う情報システムの監視及び監査

① 個人情報取扱担当者の識別及び認証

データ利活用基盤システム運用者等は、「個人情報取扱担当者の識別及び認証」として、次に掲げる措置を講じなければならない。

- 本人確認機能の整備
- 本人確認に関する情報の不正使用防止機能の整備
- 本人確認に関する情報が他人に知られないための対策

a. 手法の例示

個人情報取扱担当者の識別及び認証としては、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
本人確認機能の整備 本人確認に関する情報の不正使用防止機能の整備 本人確認に関する情報が他人に知られないための対策	パスワードを利用した認証を実施する。 ＜パスワード強度例＞ 容易に推測されないもの（8 桁以上、パスワード世代管理、3 種類以上の文字種の使用等）を設定	パスワードを利用した認証を実施する。 ・多要素認証を使用 ・生体認証を使用

b. 今回のモデル事業での具体例

- 管理区域及び取扱区域への入退室は、社員証での本人認証とアクセス制御にて入退室が管理されている。さらに個人データへアクセスする際には、パスワードを利用した認証を実施した。
- パスワードは、複雑なもの（8 桁以上、パスワード世代管理、3 種類以上の文字種の使用）を設定した。

② 個人データの管理区分の設定及びアクセス制御

データ利活用基盤システム運用者等は、「個人データの管理区分の設定及びアクセス制御」として、次に掲げる措置を講じなければならない。

- 従業者の役割・責任に応じた管理区分及びアクセス権限の設定
- 事業者内部における権限外者に対するアクセス制御
- 外部からの不正アクセスの防止措置

また、外部からの不正アクセスの防止措置として、次に掲げる措置を講じなければならない。

- アクセス可能な通信経路の限定
- 外部ネットワークからの不正侵入防止機能の整備
- 不正アクセスの監視機能の整備
- ネットワークによるアクセス制御機能の整備

a. 手法の例示

上記、措置に対する対応方法については次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
アクセス制御	個人情報取扱担当者を識別した上で、サーバ上の情報にアクセス権限のないシステム利用者は使用できないようにする。	情報を重要度別（秘、社外秘、関係者外秘等）に分類し、重要度別にシステム利用者やグループ単位（システム利用者の所属組織や役割に応じた単位）でアクセス権をつけて管理する。また、個人データにアクセスした履歴を取得する。
アクセス可能な通信経路の限定	ネットワークサービスの利用方針を策定し、社外からの通信及び、社外への通信は必要なもののみに限定する。	基本事例に加えて、通信経路を監視（通信経路の設定が要件で定めた設定になっているかを定期的に確認）する。
外部ネットワークからの不正アクセスの制御	ファイアウォールを設置し以下を実現する。 ・社内ネットワークの必要な資源のみ、社外からのアクセスを許可 ・NAT を使用し、外部に対して内部ネットワークを不可視化 ・静的ルーティング等、固定的なルーティングを制御	ファイアウォールを設置し以下を実現する。 ・社内ネットワークの一部資源のみ、社外からのアクセスを許可（必要なものを許可するのではなく、限定する） ・NAT を使用し、外部に対して内部ネットワークを不可視化 ・管理下以外のネットワーク機器に対して、ルーティング情報のフィルタを実施
不正アクセスの監視機能の整備	外部からのアクセスログを取得して、定期的に確認する。	外部からの攻撃を検出・防御する仕組み（IDS/IPS,WAF 等）を導入する。 外部からのアクセスログを取得して、定期的にレポートする。
ネットワークによるアクセス制御機能の整備	端末毎に接続制限をかける。（接続できる端末を IP にて制御する）	システム利用者毎にネットワーク使用をコントロールする。 アクセス違反に対する適切なモニタリングを実施し、異常時には自動的に警告する。

b. 今回のモデル事業での具体例

- アクセス制御は、個人データを取扱うことができる情報システム端末を限定した。また、その端末を取扱うことができる人を制限し必要最小限に留めた。
- 個人データを取扱うことができる情報システム端末から外部ネットワークへのアクセスは、必要最低限の通信に留めた。また定期的な監視も行った。
- 情報システムと外部ネットワークとの接続箇所に、ファイアウォールを設置し、上記に記載の「強化事例」を実施した。
- 不正アクセスの監視機能については WAF を使用した。
- ネットワークによるアクセス制御についても必要な通信経路のみに制限した。システム内部のサーバ間でも個人データを取扱うサーバへの通信を制限した。

③ 個人データへのアクセス権限の管理

データ利活用基盤システム運用者等は、「個人データへのアクセス権限の管理」として、次に掲げる措置を講じなければならない。

- 事業者、従業者等に対する個人データへのアクセス権限の適切な付与及び見直し
- 個人データへのアクセス権限を付与する数を必要最小限に限定
- 事業者、従業者等に付与するアクセス権限を必要最小限に限定

a. 手法の例示

上記、措置に対する対応方法については次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
システム利用者のアカウント及び、権限管理	一つのアカウントを複数のシステム利用者で使用しない。 個人データへのアクセスを可能にする権限はシステム利用者の増減や移動に伴い、アカウント及びアクセス権を変更する。 アカウント及びアクセス権を、定期的に見直す。	システム利用者の増減や移動をシステムで管理し、アカウント及びアクセス権を自動的に変更する。

b. 今回のモデル事業での具体例

- 個別アカウントごとにセキュリティルームの入室権限及び、本番サーバへのアクセス権限を付与した。（台帳管理）
- アカウントごとのアクセス権については、離任タイミングで剥奪し、必要に応じてアカウント削除を実施した。

④ 個人データの漏洩、毀損等防止策

データ利活用基盤システム運用者等は、「個人データの漏洩、既存等防止策」として、個人データの保護策を講ずるとともに、障害発生時の技術的対応・復旧手続を整備しなければならない。

① 個人データの保護策

- 蓄積個人データの漏洩防止策
- 伝送個人データの漏洩防止策
- コンピュータウイルス等不正プログラムへの防御対策

a. 手法の例示

上記措置に対する対応方法として、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
蓄積データの漏洩防止策	社外に持ち出すコンピュータ、電子媒体（USB メモリ、外付け HDD、CD/DVD 等）に対して暗号化をする。	基本事例に加え、社内コンピュータに対しても暗号化する。さらに復号時には認証が毎回必要とする。
伝送データの漏洩防止策	通信を暗号化（SSL 通信等）する。	基本事例に加え、社外に出る情報を、事前に社内で暗号化して送信する。 必要に応じて専用線にする。
暗号化強度、暗号鍵管理	電子政府推奨暗号リスト59を使用し暗号化を行う。暗号鍵を、暗号化してソフトウェア上で管理し、データの置き場所と暗号鍵の置き場所は異なる場所に配置する。	電子政府推奨暗号リストを使用し暗号化を行う。また、暗号鍵管理についてもソフトウェア上で管理し、暗号鍵の所在については、システム的な管理者以外は閲覧不可とする。
コンピュータウイルス等不正プログラムへの防御対策	ウイルス対策ソフトウェアを導入し、定期的なウィルスチェックを実施する。 ウイルス定義ファイルの更新は、1 日 1 回実施する。 悪意あるプログラムを検出・駆除及びシステムを修復した場合、システム管理者に通報する。	基本事例に加え、定期的なウイルス対策ソフトウェアでのフルスキャンを実施する。 社内の全コンピュータのウイルス対策状況を把握する仕組みを導入する。 データの改ざん対策ソフトウェア（ファイルの整合性監視ツール）を導入する。

b. 今回のモデル事業での具体例

- 蓄積データの保管は、データ自体を暗号化し保管した。また、伝送時には、ファイルの暗号化、メール送信についても専用ソフトにて伝送した。
- 暗号鍵管理は、専用サービスを利用し管理した。
- コンピュータウイルス等不正プログラムへの防御対策は、端末、管理サーバ共にセキュリティ対策ソフトを導入し、定期的なウィルスチェックを実施した。
- 悪意あるプログラムを検出・駆除した際には、システム管理者に通報するフローとした。
- データ改ざん対策ソフトウェア（ファイルの整合性監視ツール）を導入した。

② 障害発生時の技術的対応、復旧手続の整備

- 不正アクセスの発生に備えた対応、復旧手続の整備
- コンピュータウイルス等不正プログラムによる被害時の対策
- リカバリ機能の整備

[59] 総務省及び、経済産業省公表「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」を策定いたしました（最終改訂: 2020 年（令和 2 年）12 月 21 日、CRYPTREC LS-0001-2012R5）。
参照 URL: https://www.cryptrec.go.jp/list.html

c. 手法の例示

上記措置に対する対応方法として、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
・不正アクセスの発生に備えた復旧手続きの整備 ・コンピュータウイルス等不正プログラムによる被害時の対策 ・リカバリ機能の整備	バックアップのポリシー（世代管理、バックアップ対象、取得サイクル、保管場所等）を作成する。 ポリシーに従い、情報をバックアップする。 リカバリできることを定期的に確認する。	バックアップ媒体は遠隔地に保管する。 バックアップデータを、暗号化する。 リストアが、適切な時間内に可能であることを確認する。

d. 今回のモデル事業での具体例

情報システムの復旧については、過去の特定時点のシステム状態に戻す等のリカバリが問題なく行えることの手順を整備した。バックアップは日次で行った。

⑤ 個人データへのアクセスの記録及び分析

データ利活用基盤システム運用者等は、「個人データへのアクセスの記録及び分析」として、個人データへのアクセスや操作を記録するとともに、当該記録の分析・保存を行わなければならない。また、不正が疑われる異常な記録の存否を定期的に確認しなければならない。

a. 手法の例示

上記措置に対する対応方法として、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
個人データへのアクセスや操作を記録	情報システムのアクセスログを取得する。 以下、成功時の記録を残す。 アカウントによるログオンイベント(ローカル) アカウントへの管理作業 アカウント又はパスワードのポリシー変更 システムに影響のあるイベント	アカウントによるログオンイベント（ネットワーク、ドメイン、ローカル）を成功時・失敗時ともに記録する。 基本事例で取得するログについて成功時の記録だけでなく、失敗時の記録も残す。
ログの保護	ログの読み出しを必要最小限に設定する。また、ログの記録漏れ、上書き等が発生しないよう、十分な記憶容量を確保する。	基本事例に加え、短いサイクルで、別の情報システムにオンラインでログをコピー又は移動する。 暗号化して保存する。

観点	基本事例	強化事例
当該記録の分析・保存及び、不正が疑われる異常な記録の存否を定期的に確認	監視計画と監視実績に基づいた監査を実施する。 監査については、定期的に社内組織に委託する。	記録の保存に関して、保存年数、保存期間を定めて保存する。（1 年以上等） SIEM などを利用し、記録の分析をシステムで行う。 監視計画と監視実績に基づいた監査を実施する。 監査については、定期的に第三者組織に委託する。

b. 今回のモデル事業での具体例

- 個人データへのアクセスや操作の記録は、アプリ出力ログ、通信機器のログ等を取得した。また、取得したログに対して改ざんができないような設定を実施し、ログの保存自体は複数年保存できるよう設定した。
- ログの定期的な分析については、決済データを取扱っているサーバに対して、決済処理結果を精査し不正な決済の兆候がないかのチェックを実施した。

⑥ 個人データを取扱う情報システムの稼働状況の記録及び分析

データ利活用基盤システム運用者等は、「個人データを取扱う情報システムの稼動状況の記録及び分析」として、個人データを取扱う情報システムの稼動状況を記録するとともに、当該記録の分析・保存を行わなければならない。

a. 手法の例示

上記措置に対する対応方法として、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
個人データを取扱う情報システムの稼動状況の記録及び分析	情報システムが正確に稼動しているか、手動や目視、ログ記録等から確認する。	情報システムが正確に稼動しているか、自動で監視し、定期的に監視状況をレポートする。 情報システムに障害が発生した際、緊急の警告を発する。

b. 今回のモデル事業での具体例

個人データを取扱う情報システムに対し、HTTP レスポンスを監視し、500 系[60]が発生した際にアラートが上がるよう設定した。

⑦ 個人データを取扱う情報システムの監視及び監査

データ利活用基盤システム運用者等は、「個人データを取扱う情報システムの監視及び監査」として、個人データを取扱う情報システムの利用状況、個人データへのアクセ

[60] サーバ上で予期しないエラーが発生した際に返されるステータスコード
参照 URL：https://tools.ietf.org/html/rfc7231#section-6.6

ス状況及び情報システムへの外部からのアクセス状況を監視するとともに、監視システムの動作の定期的な確認等、監視状況についての点検及び監査を行わなければならない。また、セキュリティパッチの適用や情報システム固有の脆弱性の発見・その修正等、ソフトウェアに関する脆弱性対策を行わなければならない。

a. 手法の例示

上記措置に対する対応方法として、次に掲げる対応等が挙げられる。

観点	基本事例	強化事例
監視システムの動作の定期的な確認等	監視システムが正確に稼動しているか、手動、目視、ログ記録等から確認する。	監視システムが正確に稼動しているか、自動で監視し、定期的に監視状況をレポートする。 開始システムに障害が発生した際、緊急の警告を発する。
情報システムに関する脆弱性対策	セキュリティパッチ等は必要に応じて適用する。	基本事例に加え、 セキュリティパッチ等の情報を収集し、必要に応じて適用する。 ぜい弱性検査ツールによる検査を定期的に実施する。

b. 今回のモデル事業での具体例

- 監視システム（ファイアウォール、IDS/IPS、ファイル整合性監視、アンチウイルス等）の動作確認は、監視機能のヘルスチェックを実施した。
- セキュリティパッチの適用についても緊急度に応じて随時実施した。
- 情報システムの脆弱性診断を内部監査にて行った。

5.4 安全管理措置の内容（データ利活用推進主体及び、データ分析者向け）

本節では、データ利活用推進主体及びデータ分析者向けに、データ保護のために必要な安全管理措置を記載する。決済データの生データを持たず、加工されたデータしか持たないこれらの事業者においては、その保有するデータの内容によって適切な安全管理措置を講じる必要がある。決済データが十分に加工され、これらの事業者において特定の個人を識別できず、容易照合性がないのであれば、個人情報に該当しない。個人情報保護法上の安全管理措置義務を負わない場合もあるが、加工の程度によっては、引き続き個人情報に該当し安全管理措置義務を負う場合もある。ただし、これらの線引きは明確ではないことも多いため、本書においては通常の個人データについての安全管理措置として、「個人情報の保護に関する法律のガイドライン(通則編)」8.（別添)講ずべき安全管理措置の内容を参考に安全管理措置を講じることを推奨する。データ利活用基盤システム運用者が保有する決済データの生データと比較すると、データ利活用推進主体及びデータ分析者が保有するデータは、リスクが低い状態のデータになって

いることを想定しており、前節において紹介した安全管理措置よりも軽い措置で足りる場合が多いと考えられる。

以下、「個人情報の保護に関する法律のガイドライン(通則編)」の「8. (別添)講ずべき安全管理措置」[61]の内容となる。

5.4.1 個人データの安全管理に関する基本方針の策定

個人情報取扱事業者は、個人データの適正な取扱いの確保について組織として取り組むために、基本方針を策定することが重要である。

5.4.2 個人データの取扱いに係る規律の整備

個人情報取扱事業者は、その取扱う個人データの漏えい等の防止その他の個人データの安全管理のために、個人データの具体的な取扱いに係る規律を整備しなければならない。

5.4.3 実施体制の整備に関する組織的安全管理措置

個人情報取扱事業者は、組織的安全管理措置として、次に掲げる措置を講じなければならない。

① 組織体制の整備

安全管理措置を講ずるための組織体制を整備しなければならない。

② 個人データの取扱いに係る規律に従った運用

あらかじめ整備された個人データの取扱いに係る規律に従って個人データを取り扱わなければならない。なお、整備された個人データの取扱いに係る規律に従った運用の状況を確認するため、利用状況等を記録することも重要である。

③ 個人データの取扱状況を確認する手段の整備

個人データの取扱状況を確認するための手段を整備しなければならない。

④ 漏えい等の事案に対応する体制の整備

漏えい等の事案の発生又は兆候を把握した場合に適切かつ迅速に対応するための体制を整備しなければならない。なお、漏えい等の事案が発生した場合、二次被害の防止、

---

[61] 個人情報保護委員会公表の現行版（平成 28 年 11 月公表、令和 3 年 1 月一部改正）P86 以降に「8（別添）講ずべき安全管理措置の内容」が記載されている。
具体的な内容については、各項目ごとに記載されている「手法の例示」を参照されたい。
参照 URL：https://www.ppc.go.jp/files/pdf/210101_guidlines01.pdf

類似事案の発生防止等の観点から、事案に応じて、事実関係及び再発防止策等を早急に公表することが重要である（※）。

（※）個人情報取扱事業者において、漏えい等の事案が発生した場合等の対応の詳細については、「個人データの漏えい等の事案が発生した場合等の対応」[62]について参照。

⑤　取扱状況の把握及び安全管理措置の見直し

個人データの取扱状況を把握し、安全管理措置の評価、見直し及び改善に取り組まなければならない。

5.4.4 人的安全管理措置

個人情報取扱事業者は、人的安全管理措置として、次に掲げる措置を講じなければならない。また、個人情報取扱事業者は、従業者に個人データを取扱わせるにあたっては、法第 21 条に基づき従業者に対する監督をしなければならない。

①　従業者の教育

従業者に、個人データの適正な取扱いを周知徹底するとともに適切な教育を行わなければならない。

5.4.5 物理的安全管理措置

個人情報取扱事業者は、物理的安全管理措置として、次に掲げる措置を講じなければならない。

①　個人データを取り扱う区域の管理

個人情報データベース等を取扱うサーバやメインコンピュータ等の重要な情報システムを管理する区域（以下「管理区域」という。）及びその他の個人データを取扱う事務を実施する区域（以下「取扱区域」という。）について、それぞれ適切な管理を行わなければならない。

②　機器及び電子媒体等の盗難等の防止

個人データを取扱う機器、電子媒体及び書類等の盗難又は紛失等を防止するために、適切な管理を行わなければならない。

---

[62] 「個人データの漏えい等の事案が発生した場合等の対応について（平成 29 年個人情報保護委員会告示第 1 号）」
参照 URL：https://www.ppc.go.jp/files/pdf/iinkaikokuzi01.pdf

③　電子媒体等を持ち運ぶ場合の漏えい等の防止

個人データが記録された電子媒体又は書類等を持ち運ぶ場合、容易に個人データが判明しないよう、安全な方策を講じなければならない。

なお、「持ち運ぶ」とは、個人データを管理区域又は取扱区域から外へ移動させること又は当該区域の外から当該区域へ移動させることをいい、事業所内の移動等であっても、個人データの紛失・盗難等に留意する必要がある。

④　個人データの削除及び機器、電子媒体等の廃棄

個人データを削除し又は個人データが記録された機器、電子媒体等を廃棄する場合は、復元不可能な手段で行わなければならない。

また、個人データを削除した場合、又は、個人データが記録された機器、電子媒体等を廃棄した場合には、削除又は廃棄した記録を保存することや、それらの作業を委託する場合には、委託先が確実に削除又は廃棄したことについて証明書等により確認することも重要である。

5.4.6 技術的安全管理措置

個人情報取扱事業者は、情報システム（パソコン等の機器を含む。）を使用して個人データを取扱う場合（インターネット等を通じて外部と送受信等する場合を含む。）、技術的安全管理措置として、次に掲げる措置を講じなければならない。

①　アクセス制御

担当者及び取扱う個人情報データベース等の範囲を限定するために、適切なアクセス制御を行わなければならない。

②　アクセス者の識別と認証

個人データを取扱う情報システムを使用する従業者が正当なアクセス権を有する者であることを、識別した結果に基づき認証しなければならない。

③　外部からの不正アクセス等の防止

個人データを取扱う情報システムを外部からの不正アクセス又は不正ソフトウェアから保護する仕組みを導入し、適切に運用しなければならない。

④　情報システムの使用に伴う漏えい等の防止

情報システムの使用に伴う個人データの漏えい等を防止するための措置を講じ、適切に運用しなければならない。

6 用語集

用語	読み方	意味
IDS/IPS	あいでぃーえす／あいぴーえす	IDS は侵入検知システム（Intrusion Detection System）の略であり、IPS は侵入防止システム（Intrusion Prevention System）の略。インターネットに接続されたネットワークやサーバを不正侵入から防御するためのシステム。IDS の役割が不正なアクセスの検知や通知にとどまるのに対し、IPS は侵入検知システムの機能に加えて、不正なパケットを自動的に遮断する機能を持つ。 出典：総務省「国民のための情報セキュリティサイト」
暗号鍵管理	あんごうかぎかんり	暗号鍵（データを暗号化するときに使われる鍵のこと）の適切な管理を指す。 出典：総務省「国民のための情報セキュリティサイト」
アンチウイルス	あんちういるす	ウイルス、ワーム、トロイ（またはトロイの木馬）、スパイウェア、アドウェア、ルートキットなど、様々な形式の悪意のあるソフトウェア（「マルウェア」とも呼ばれる）を検出、除去し、これらのソフトウェアからコンピュータを保護するプログラム（ソフトウェア）のこと。 出典：Payment Card Industry （PCI） データセキュリティ基準（DSS） 、及び、ペイメントアプリケーション データセキュリティ基準（PA-DSS） 用語集
片側認証	かたがわにんしょう	複数の組織間等で、システムを構築する場合、相互の正当性や、認証を確認するレベルがあり、関連する人や組織、モノの対において、片側だけが相手を認証すること。 出典：DFFT(Data Free Flow With Trust）実現のためのアーキテクチャ設計と国際標準化推進の研究開発
決済事業者	けっさいじぎょうしゃ	店舗に決済手段を提供している企業のこと。本書ではバーコード・QR コード決済を提供している事業者を指す。
決済データ	けっさいでーた	本書では、決済取引が発生した際に、店舗から決済事業者に送信した決済入力データ、及び決済事業者から店舗へ決済処理結果を返答する決済取引データを総称して決済データと呼称する。「いつ」、「どの店舗で」、「誰が」、「いくら」使ったのか知ることが可能である。
決済取引データ	けっさいとりひきでーた	本書では、地域利用者が店舗で決済を行う際、決済事業者側の決済処理で発生するデータ（決済結果などもここには含まれる）を決済取引データと呼称する。
決済入力データ	けっさいにゅうりょくでーた	本書では、地域利用者が店舗で決済を行う際、決済事業者へ決済を依頼するデータを決済入力データと呼称する。

用語	読み方	意味
購買データ	こうばいでーた	本書では、店舗側で生成する購買取引データを指す。「いつ」、「どの店で」、「誰が」、「どの商品を」、「いくつ」、「いくらで」購入したのかを含むデータである。購入商品名、単価、購入数等が含まれる。
SIEM	しーむ	Security Information and Event Management の略。サーバやネットワーク機器、セキュリティ関連機器、アプリケーション等から集められたログ情報に基づいて、異常があった場合に管理者に通知したり対策を知らせたりする仕組み。 出典：企業における情報システムのログ管理に関する実態調査-調査報告書
JPQR	じぇいぴーきゅーあーる	総務省が経済産業省と連携して、一般社団法人キャッシュレス推進協議会が策定した決済用統一 QR コード・バーコード」のこと。 出典：2020 年度総務省統一 QR[JPQR]普及事業ホームページ
情報システム	じょうほうしすてむ	ハードウェア及びソフトウェアから成るシステムであって、情報処理又は通信の用に供するものをいう。 出展：政府機関等の情報セキュリティ対策のための統一基準（平成 30 年度版）
スマートフォンアプリ	すまーとふぉんあぷり	スマートフォンやタブレット等で動作するように設計・制作されたアプリケーションソフトウエアをいう。コミュニケーション、動画・音楽視聴、地図・ナビゲーション、電子書籍、ネットショッピング、ゲーム用のアプリなどが代表的。 出展：総務省「情報通信白書（平成 28 年度版）」
脆弱性検査ツール	ぜいじゃくせいけんさつーる	コンピュータやネットワークにおいて、情報セキュリティ上の問題となる可能性がある弱点を検査するツールをいう。ツールにはいくつか種類が存在するが、ツール内にウェブアプリケーションの脆弱性を検査する検査コードが複数用意されており、ツールが自動的に検査コードの送信やレスポンスの解析を行い、脆弱性の有無を判別するようなものを指す。 出典：IPA テクニカルウォッチ「ウェブサイトにおける脆弱性検査手法(ウェブアプリケーション検査編)」
静的ルーティング	せいてきるーてぃんぐ	ネットワーク経路を手動で設定したもので、予め最適な経路を固定的に定義すること。 ルートが固定化されるためトラブルが発生した時に追跡が容易になるなどのメリットはあるが、ネットワークが変更されるたびにルーティングテーブルの設定を変更する必要がある。 出典：Linux のシステム管理に関する知識Ⅱ（独立行政法人 情報処理推進機構）
セキュリティパッチ	せきゅりてぃぱっち	OS やサービスにバグや脆弱性が発見された場合に、ベンダーまたはセキュリティコミュニティからリリースされるアドバイザリとそれらを修正するためのプログラム（パッチ）のこと。 出典：セキュアな Web サーバーの構築と運用（独立行政法人 情報処理推進機構）

用語	読み方	意味
相互認証	そうごにんしょう	複数の組織間等でシステムを構築する場合、相互の正当性や、認証を確認するレベルがあり、関連する人や組織、モノが相互に相手を認証すること。 出典：DFFT(Data Free Flow With Trust）実現のためのアーキテクチャ設計と国際標準化推進の研究開発
多要素認証	たようそにんしょう	アクセス権限を得るために必要な本人確認を行う際に、複数種類の要素（証拠）をユーザに要求する認証方式のこと。認証するための要素を大別すると、「記憶」、「所持」、「生体情報」の 3 つがあり、そのうち 2 つの要素で認証することを二要素認証、2 つ以上の要素で認証することを多要素認証という。 出典:情報セキュリティ 10 大脅威 2020～セキュリティ対策は一丸となって、Let's　Try!!～（独立行政法人情報処理推進機構）
地域ウォレット	ちいきうぉれっと	本書では、地域ウォレットとは、エンドユーザにとってはその地域の中での暮らしや体験のために身近にあると役に立つものが「財布」のようにまとめて管理されているスマートフォンアプリケーションと定義している。 地域ウォレットを活用して、決済データ、購買データ、利用者属性データを紐付け地域活性化や社会課題解決に利活用することが可能である。
データ	でーた	情報の表現であって、伝達、解釈または処理に適するように形式化され、再度情報として解釈できるもの。 出典：ISO/IEC 2382-1,JIS X0001 情報処理用語-基本用語
データ利活用基盤	でーたりかつようきばん	本書では、利用者属性データ、決済データ、購買データを集約し、データ利活用のためのデータを保管・管理するシステム基盤のことを指す。
電子政府推奨暗号リスト	でんしせいふすいしょうあんごうりすと	暗号技術検討会及び関連委員会（以下、CRYPTREC という。）により安全性及び実装性能が確認された暗号技術について、市場における利用実績が十分であるか、又は、今後の普及が見込まれると判断され、当該技術の利用を推奨するもののリストのこと。 出典：総務省及び経済産業省 「電子政府における調達のために参照すべき暗号のリスト(CRYPTREC 暗号リスト)」
NAT	なっと	ネットワークアドレス変換（Network Address Translation）の略。ネットワークマスカレードまたは IP　マスカレードと呼ばれる。1 つのネットワーク内で使用されている IP アドレスを別のネットワーク内で知られている異なる IP　アドレスに変更し、組織内から内部的に見える内部アドレスと外部でのみ見える外部アドレスを持つことを可能にする。 出典：Payment Card Industry （PCI） データセキュリティ基準（DSS） およびペイメントアプリケーション データセキュリティ基準（PA-DSS）　用語集
パスワード世代管理	ぱすわーどせだいかんり	過去に使ったパスワードの使いまわしを抑止するために、過去に設定したパスワードを世代管理することを指す。

用語	読み方	意味
ファイアウォール	ふぁいあうぉーる	外部のネットワークと内部のネットワークを結ぶ箇所に導入することで、外部からの不正な侵入を防ぐことができるシステムのこと。またはシステムが導入された機器。 出典：総務省「国民のための情報セキュリティサイト」
ファイル整合性監視	ふぁいるせいごうせいかんし	特定のファイルまたはログを監視して、変更された場合にそれを検出する技術またはテクノロジのこと。重要なファイルまたはログが変更された場合、該当するセキュリティ担当者に警告を送信する。 出典：Payment Card Industry （PCI） データセキュリティ基準（DSS） およびペイメントアプリケーション データセキュリティ基準（PA-DSS） 用語集
ヘルスチェック	へるすちぇっく	本書では、Web サーバのヘルスチェックのことを指し、実際にコンテンツにアクセスし、その機能の稼働状態をチェックする。
包括加盟店契約	ほうかつかめいてんけいやく	本書では、決済事業者に代わり、データ利活用基盤システム運用者もしくは、データ利活用推進主体が加盟店開拓、加盟店管理を行う契約方式のことを指す。
リストア	りすとあ	ハードディスクなどの記憶装置が破損するなどしてデータが失われた際に、予め取得しておいたデータの複製を書き戻すなどして復元すること。
利用者属性データ	りようしゃぞくせいでーた	本書では、地域利用者個人の属性データのことを指す。地域ウォレット利用登録時に、アプリから地域利用者によって入力されるデータ等が対象となる。
WAF	わふ	Web Application Firewall の略。ウェブアプリケーションの脆弱性を悪用した攻撃などからウェブアプリケーションを保護するソフトウェア、またはハードウェアのこと。WAF は脆弱性を修正するといったウェブアプリケーションの実装面での根本的な対策ではなく、攻撃による影響を低減する対策となる。 出典：Web Application Firewall 読本（独立行政法人情報処理推進機構）